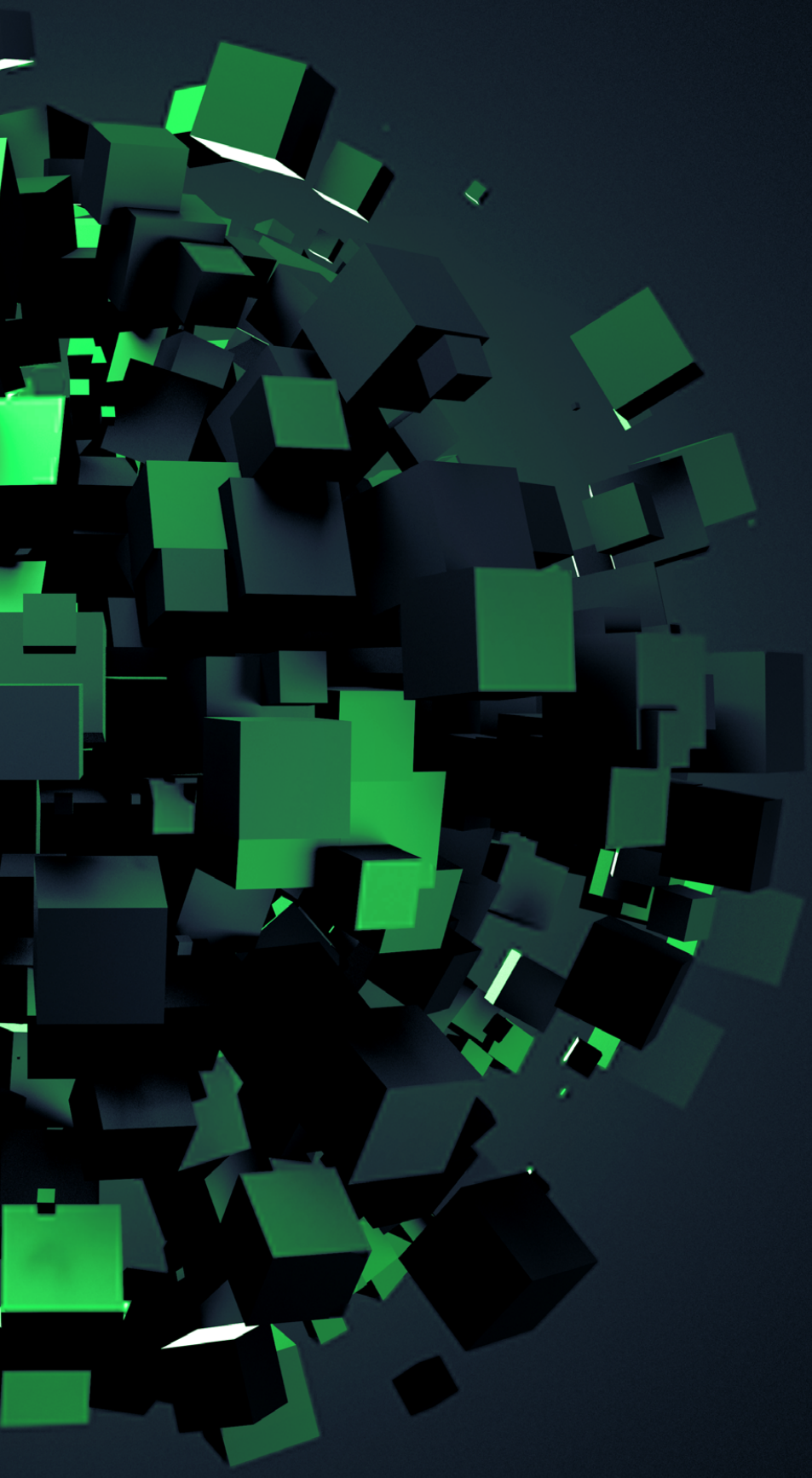
Incydenty i zagrożenia



Przegląd nowych kampanii

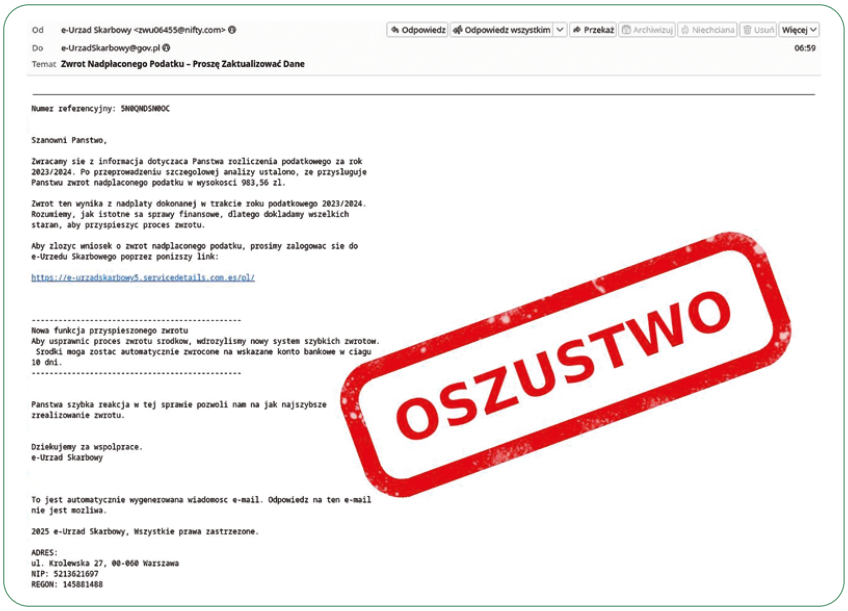
Krajobraz zagrożeń w polskiej cyberprzestrzeni nieustannie ewoluuje. Przestępcy systematycznie doskonalą swoje metody, a ich kampanie stają się coraz trudniejsze do odróżnienia od autentycznej korespondencji. Wśród utrwalonych schematów ataków dominują kampanie phishingowe ukierunkowane na kradzież haseł do kont poczty elektronicznej oraz serwisów społecznościowych. Niezmiennie wysoką aktywność wykazują również fałszywe witryny podszywające się pod serwisy rządowe i dostawców usług kurierskich, w szczególności pod Pocztę Polską oraz InPost.

W dalszej części rozdziału przedstawiliśmy przegląd najczęściej występujących kampanii w 2025 roku wraz z opisem technik stosowanych przez oszustów oraz potencjalnych konsekwencji dla użytkowników.

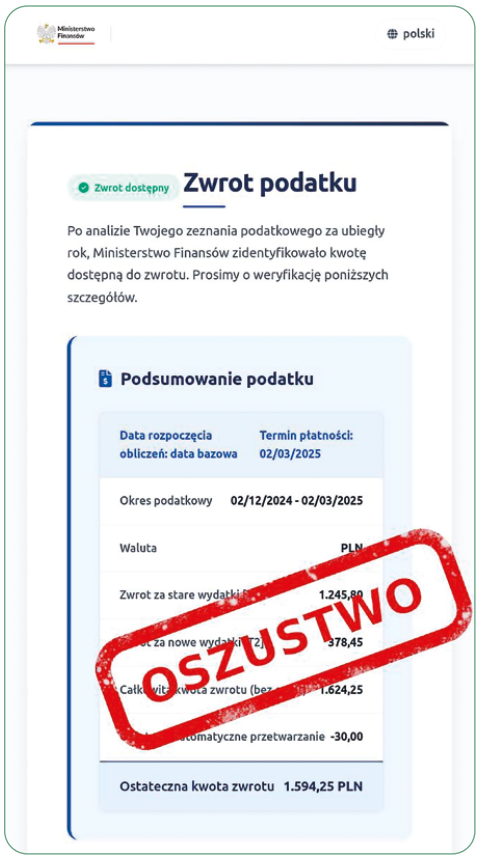
Zwrot podatku – e-Urząd Skarbowy oraz KAS

Jednym z najpopularniejszych scenariuszy phishingowych pozostaje obietnica zwrotu podatku. Przestępcy wykorzystują wizerunek Ministerstwa Finansów, rozsyłają wiadomości e-mail o rzekomym zwrocie oczekującym na zatwierdzenie. Komunikaty charakteryzują się profesjonalnym wyglądem naśladującym oficjalną korespondencję instytucji państwowych, co zwiększa ich wiarygodność. Wiadomości zawierają odnośnik do fałszywej strony imitującej portal rządowy. Pod pretekstem finalizacji procedury zwrotu strona wyłudza dane logowania do bankowości elektronicznej i dane karty płatniczej. Przechwycone dane umożliwiają sprawcom przejęcie kont bankowych ofiar oraz dokonywanie transakcji w ich imieniu.

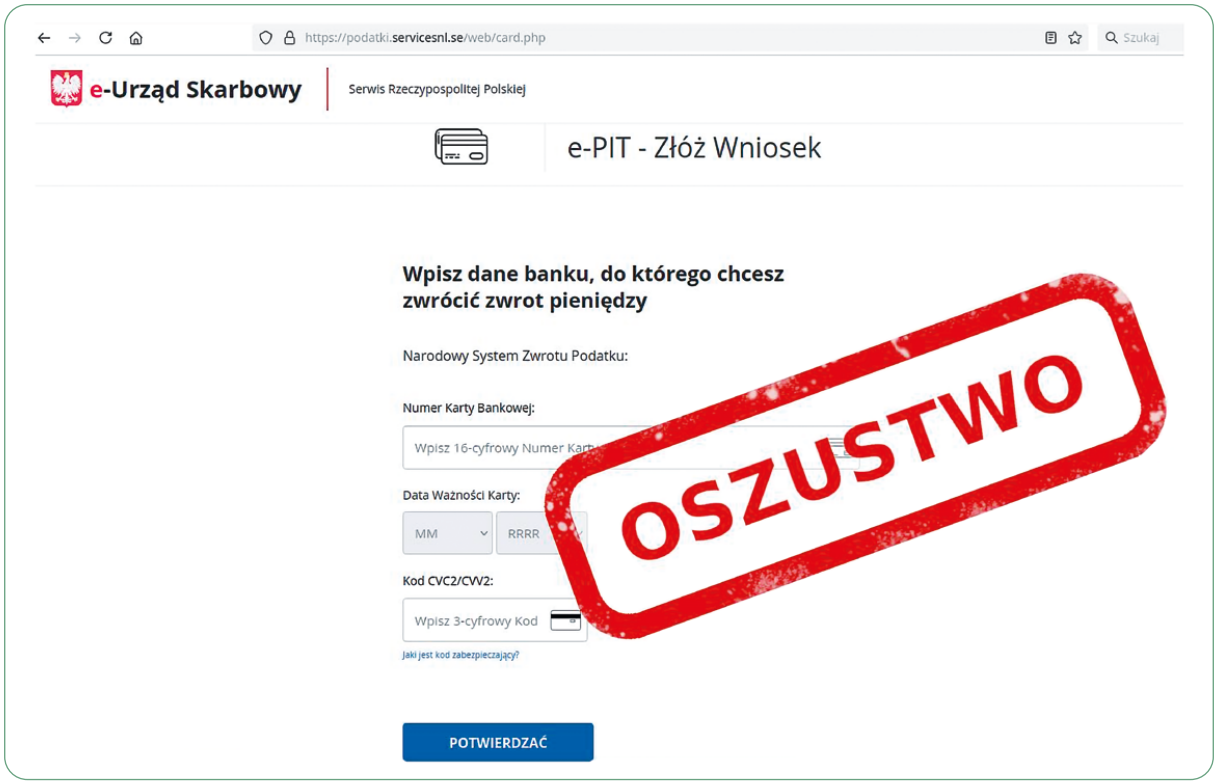
RYSUNEK 1. Fałszywa wiadomość informująca o zwrocie nadpłaconego podatku



RYSUNEK 2. Przykład oszustwa na zwrot podatku



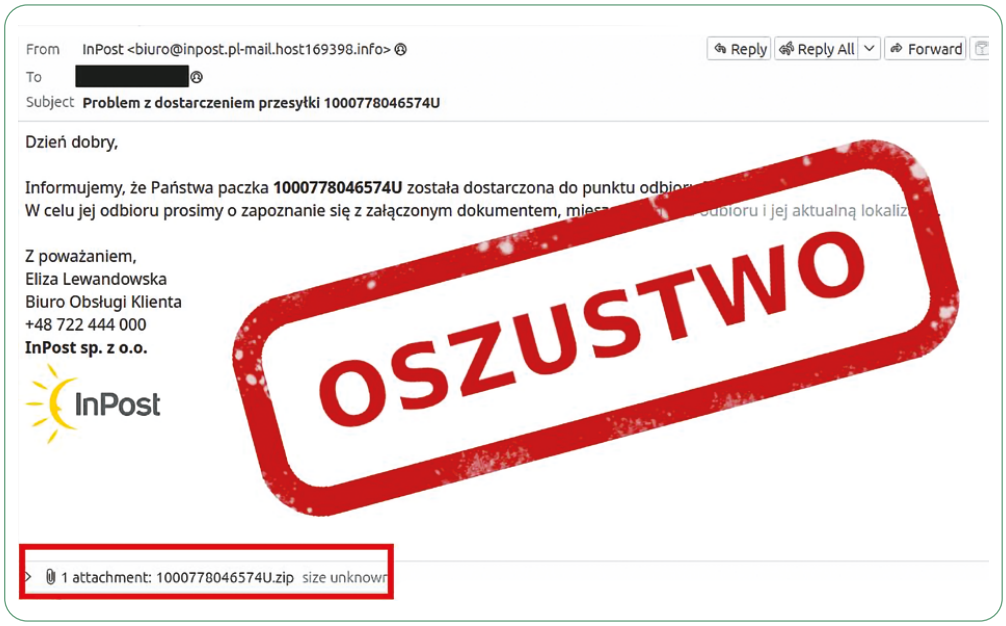
RYSUNEK 3. Fałszywa strona służąca do wyłudzania danych karty płatniczej



Niedostarczone paczki – InPost, Poczta Polska, e-Doręczenia

Popularność zakupów internetowych sprawia, że wiadomości dotyczące przesyłek kurierskich są skuteczną przynętą wykorzystywaną przez cyberprzestępców. Szczególnie często podszywają się oni pod firmę InPost. W fałszywych wiadomościach e-mail informują o rzekomych problemach z doręczeniem przesyłki i nakłaniają odbiorcę do pobrania i uruchomienia załącznika. Załącznik zawiera złośliwy skrypt, który po uruchomieniu instaluje na urządzeniu ofiary szkodliwe oprogramowanie. Umożliwia ono kradzież haseł do kont poczty elektronicznej, a ponadto wykorzystuje moc obliczeniową zainfekowanego urządzenia do wydobywania kryptowalut (tzw. cryptojacking).

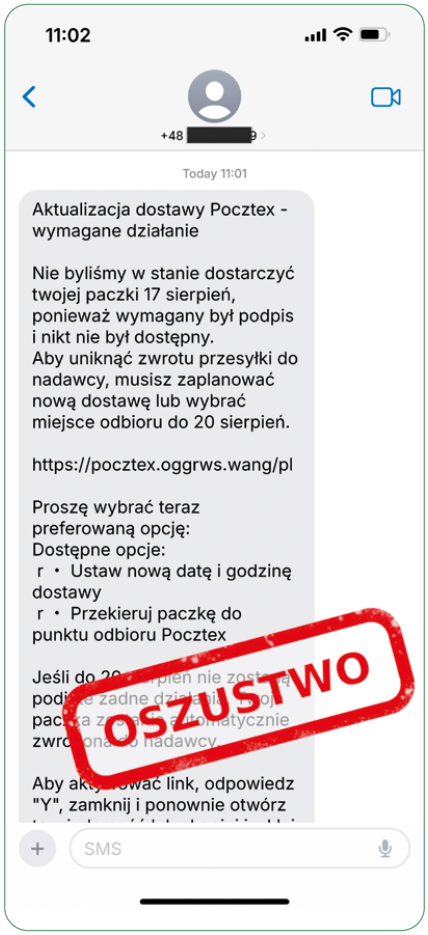
RYSUNEK 4. Fałszywa wiadomość, w której oszuści informują odbiorcę o problemie z dostarczeniem przesyłki



Oprócz wiadomości e-mail przestępcy wykorzystują także kanał SMS. Oszukańcze wiadomości tekstowe informują o fikcyjnych problemach z doręczeniem przesyłki i kierują odbiorców do witryn phishingowych imitujących strony popularnych firm kurierskich w celu wyłudzenia danych osobowych oraz informacji o kartach płatniczych.

Szczególnie ciekawy jest wariant kampanii omijający wbudowane zabezpieczenia telefonów przed otwieraniem linków od nieznanych nadawców. Nakłonienie odbiorcy do wysłania odpowiedzi na wiadomość powoduje aktywację zawartego w niej odnośnika i ułatwia przejście do strony phishingowej. To pokazuje, jak przestępcy zmieniają swój sposób działania w odpowiedzi na wprowadzanie nowych mechanizmów bezpieczeństwa.

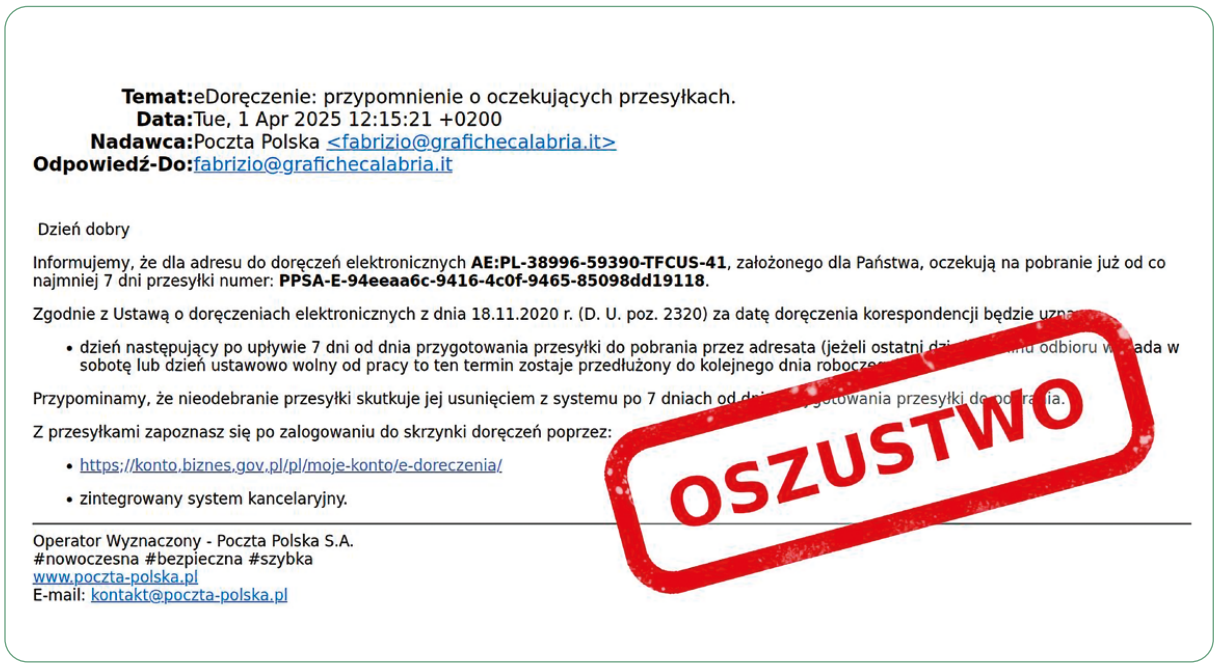
RYSUNEK 5. Przykład fałszywej wiadomości SMS, w której oszuści nakłaniają użytkownika do wysłania odpowiedzi



Wraz z rosnącą popularnością usług cyfrowej administracji pojawiły się kampanie podszywające się pod system e-Doręczeń. Sfałszowane wiadomości e-mail informują o nieodebranej przesyłce urzędowej i zawierają ostrzeżenie o jej usunięciu w razie braku reakcji w określonym terminie.

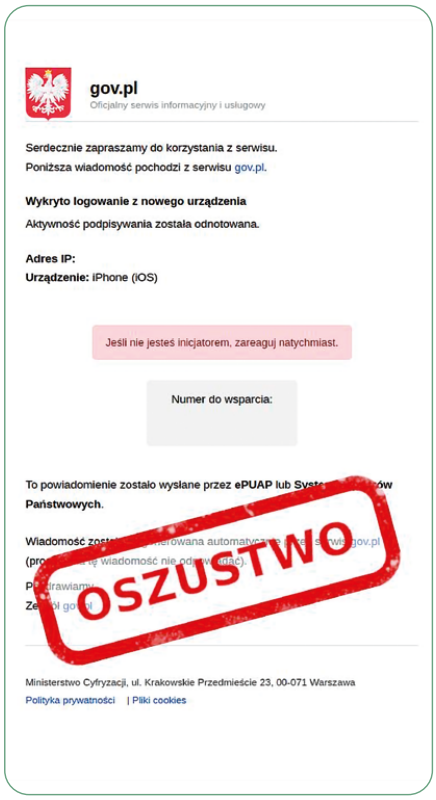
Komunikaty zawierają odnośnik do witryny imitującej portal biznes.gov.pl, na której wyłudzane są dane logowania do kont poczty elektronicznej. Kampania wykorzystuje poczucie pilności – groźba usunięcia dokumentów ma skłonić odbiorcę do natychmiastowego działania bez weryfikacji, czy wiadomość jest autentyczna.

RYSUNEK 6. Fałszywa wiadomość z linkiem do strony wyłudzającej dane logowania do poczty elektronicznej



Sprawy urzędowe – serwisy w domenie gov.pl

Serwisy rządowe w domenie gov.pl cieszą się wysokim zaufaniem społecznym, dlatego przestępcy często wykorzystują ich wizerunek w swoich kampaniach. Rozsyłane wiadomości występują w kilku wariantach: powiadomienia o oczekującej korespondencji urzędowej, o wykrytej aktywności na koncie użytkownika lub o zarejestrowaniu sesji na nieznanym urządzeniu mobilnym.

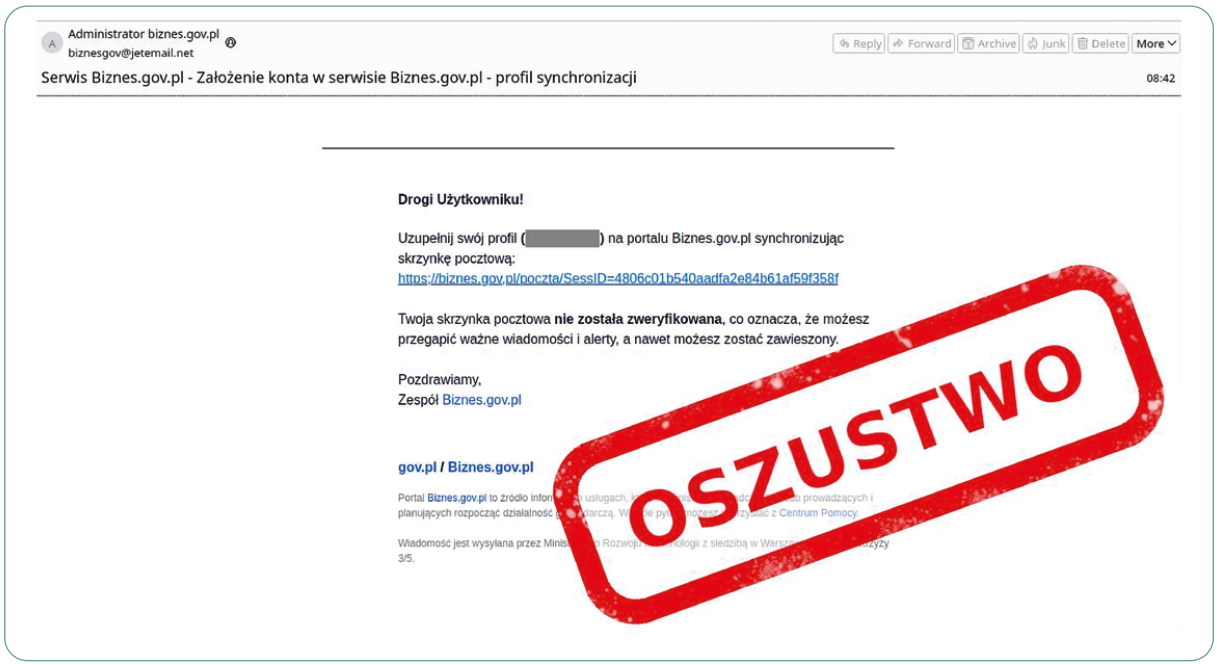


Wspólnym elementem wszystkich wariantów jest próba nakłonienia odbiorcy do nawiązania kontaktu telefonicznego pod wskazanym numerem. W trakcie rozmowy sprawcy stosują różne techniki manipulacji, aby skłonić ofiarę do instalacji oprogramowania umożliwiającego zdalny dostęp do jej komputera.

Przejęcie kontroli nad urządzeniem pozwala atakującym na wykonywanie przelewów z konta ofiary, co prowadzi do utraty zgromadzonych środków.

RYSUNEK 7. Fałszywa wiadomość informująca o nowej sesji na nieznanym urządzeniu mobilnym

RYSUNEK 8. Fałszywa wiadomość, w której oszuści nakłaniają użytkownika do synchronizacji skrzynki pocztowej

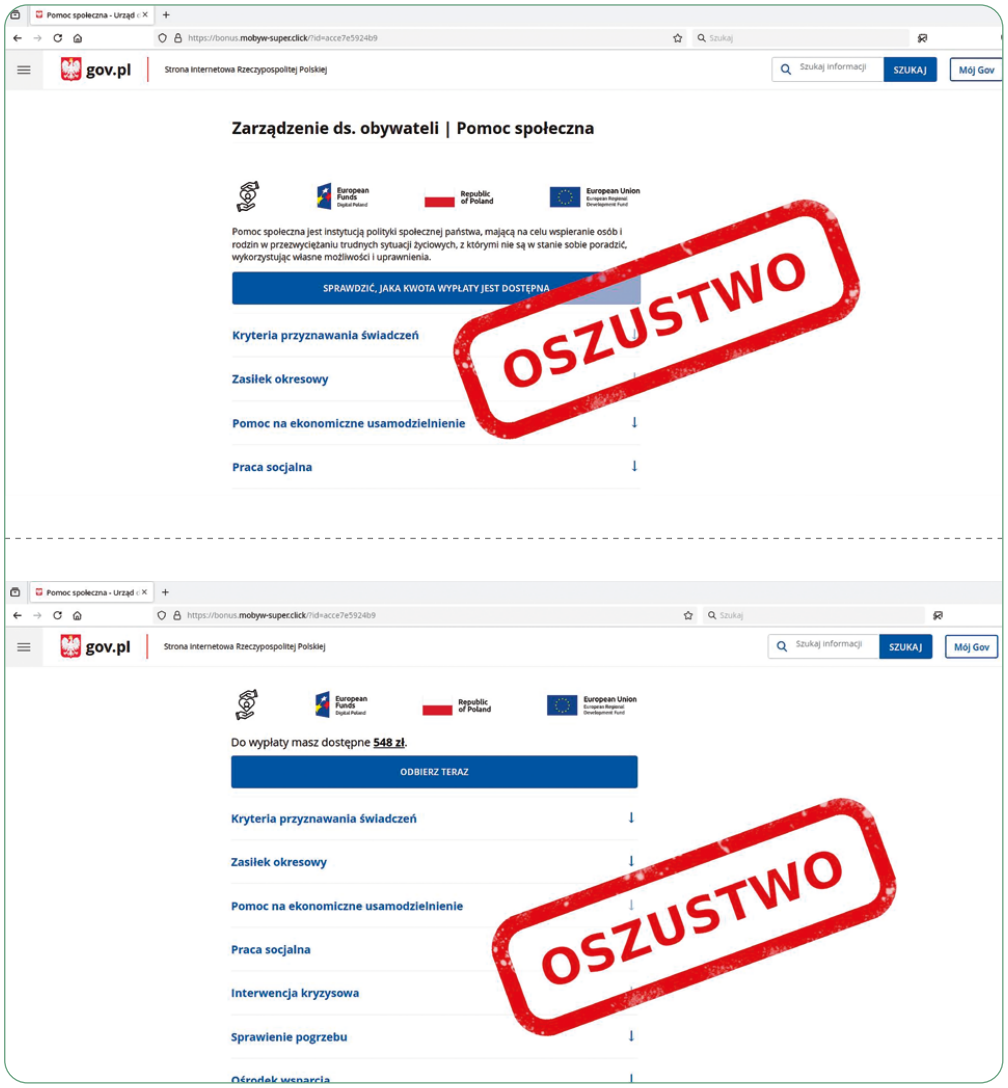


Weryfikacja uprawnień do świadczeń socjalnych

Obietnica łatwego dostępu do świadczeń socjalnych to kolejny skuteczny scenariusz oszustwa. W mediach społecznościowych rozpowszechniane są oszukańcze reklamy oferujące sprawdzenie uprawnień do dodatkowych wypłat. Reklamy kierują użytkowników do witryn imitujących portal gov.pl, gdzie jedynym wymaganym krokiem jest podanie numeru PESEL.

Po wprowadzeniu numeru PESEL następuje przekierowanie do strony podszywającej się pod operatora płatności Przelewy24, zawierającej sfałszowane formularze logowania do bankowości internetowej. Przechwycone dane logowania umożliwiają dostęp do rachunków bankowych ofiar i kradzież środków.

RYSUNEK 9. Fałszywa strona podszywająca się pod portal gov.pl, na której można rzekomo sprawdzić przysługujące świadczenia socjalne

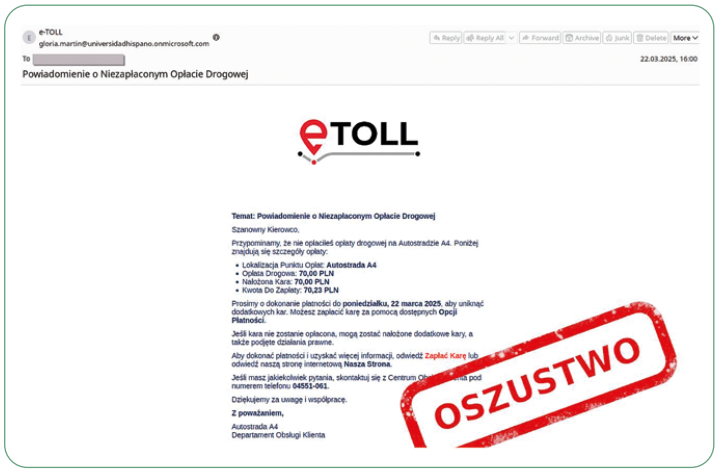


Opłata e-TOLL

Oszukańcze wiadomości dotyczące systemu e-TOLL trafiają na podatny grunt wśród kierowców. Komunikaty informują o rzekomym nieuregulowaniu opłaty za przejazd i zawierają odnośnik do strony naśladującej oficjalny serwis.

Strona zawiera dwuetapowy mechanizm wyłudzenia danych. Pierwszy formularz służy do pozyskania danych osobowych ofiary, w tym numeru dowodu osobistego. Drugi przechwytuje dane karty płatniczej wraz z kodem CVV/CVC. Pozyskane informacje umożliwiają sprawcom kradzież pieniędzy z konta ofiary.

RYSUNEK 10. Fałszywe powiadomienie o niezapłaconej opłacie drogowej



Urząd Statystyczny

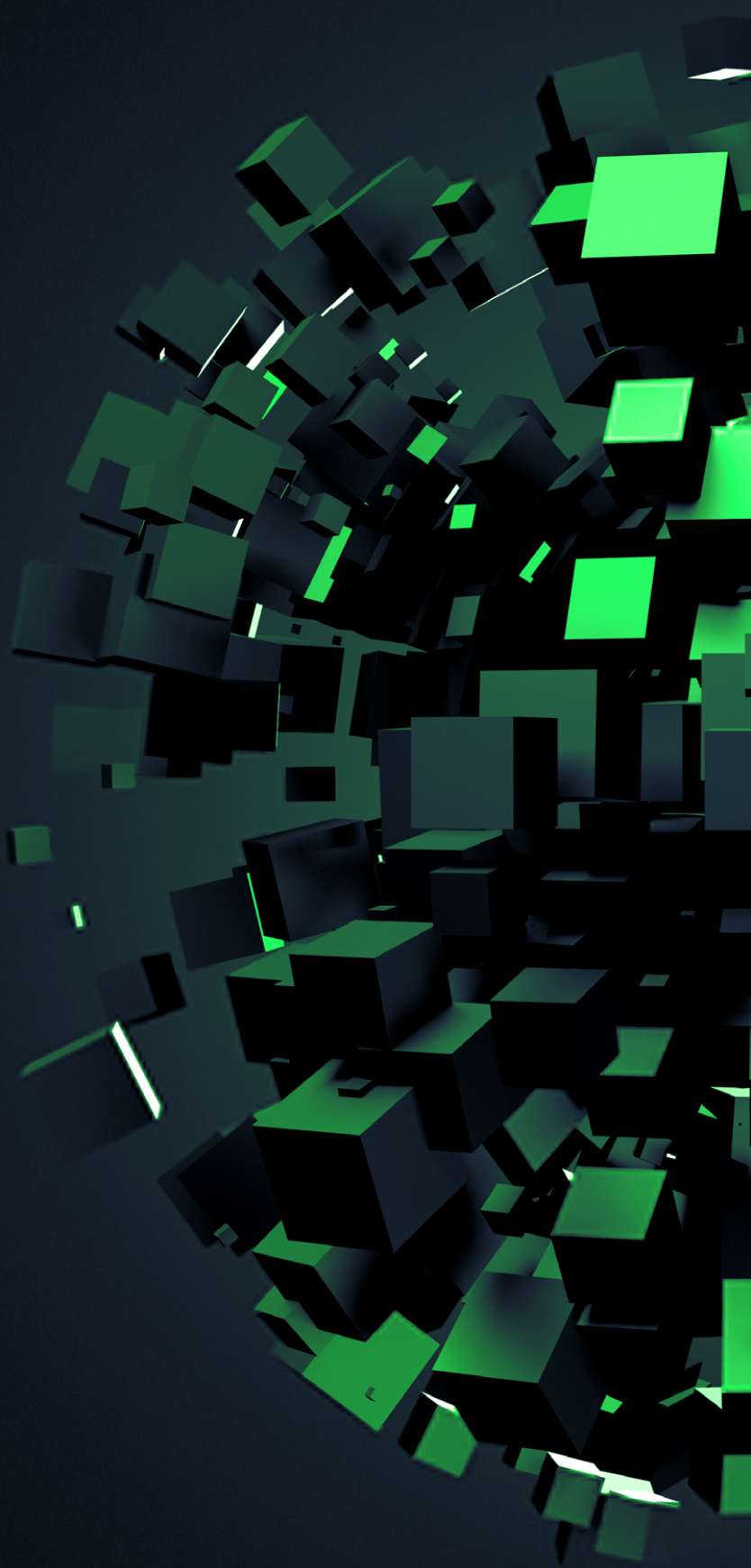
Przestępcy wykorzystują także nazwę Urzędu Statystycznego w Warszawie. Rozsyłane wiadomości e-mail informują o fikcyjnym obowiązku uzupełnienia dokumentacji i zawierają złośliwy załącznik.

Wiarygodność komunikatów jest wzmacniana dzięki profesjonalnej strukturze wiadomości, łącznie ze szczegółową stopką, która pojawia się w oficjalnej korespondencji instytucji publicznej. Załącznik zawiera oprogramowanie typu RAT (ang. Remote Access Trojan – trojan umożliwiający zdalny dostęp), które po uruchomieniu pozwala sprawcom przejąć kontrolę nad komputerem ofiary. Złośliwe oprogramowanie wykrada zapisane hasła i inne poufne dane przechowywane na zainfekowanym urządzeniu.

RYSUNEK 11. E-mail zawierający złośliwy załącznik – przykład wykorzystania wizerunku Urzędu Statystycznego w Warszawie



Działania CERT Polska



Lista Ostrzeżeń

W 2025 roku Lista Ostrzeżeń pobiła kolejny rekord. Setki tysięcy szkodliwych domen blokowanych przez CERT Polska pokazuje, jak ważnym jest ona narzędziem.

Obecnie utrzymywana jest druga wersja Listy Ostrzeżeń. Domeny umieszczane są na niej na okres 6 miesięcy od momentu analizy, a w przypadku dalszego utrzymywania szkodliwych treści domena zostaje ponownie wpisana na Listę. W porównaniu z pierwszą wersją, w której domeny były umieszczane na stałe, takie rozwiązanie pomaga ograniczyć rozmiar pliku, a także koncentruje się na aktualnych zagrożeniach i kampaniach obserwowanych przez nasz zespół. Widzimy, że domeny wykorzystywane są krótko, ale za to na szeroką skalę. Poprawna implementacja Listy Ostrzeżeń pozwala blokować takie zagrożenie w ciągu 5 minut od dodania domen przez nasz zespół.

Informacje o szkodliwych domenach zbierane są za pośrednictwem kilku kanałów, z których jednym z najczęściej wykorzystywanych nadal pozostaje numer 8080. Łatwość zgłoszenia poprzez przekazanie podejrzanego SMS-a na ten numer powoduje, że jest to często wybierana forma przesyłania nam stron do analizy, szczególnie tych, które otrzymali Państwo właśnie w wiadomości SMS. Zgłoszenia dotyczące podejrzanych stron internetowych czy wiadomości e-mail wysyłane są także m.in. za pomocą formularza dostępnego na stronie incydent.cert.pl czy przez aplikację mObywatel w ramach usługi Bezpiecznie w sieci. Na podstawie danych z tych źródeł, danych własnych i przekazanych przez naszych partnerów oraz po naszej analizie na Listę Ostrzeżeń w 2025 roku trafiło prawie 245 tys. domen.

Łatwość korzystania z Listy Ostrzeżeń połączona z jej wysoką skutecznością przyciąga użytkowników. Obserwujemy to na podstawie liczby pobrań, która w 2025 roku wyniosła prawie 1,3 mld, co przełożyło się na zablokowanie ok. 141,1 mln wejść na niebezpieczne strony. Oznacza to wzrost w stosunku do 2024 roku odpowiednio o 273% i 96,5%.

Dziękujemy wszystkim zgłaszającym oraz nieustająco zachęcamy do przesyłania nam podejrzanych linków, domen oraz SMS-ów także w 2026 roku.

Walka z oszustwami SMS

Od lat jednym z najpopularniejszych sposobów dotarcia do potencjalnych ofiar oszustwa są wiadomości SMS. Każdy z nas ma telefon niemal zawsze przy sobie, natychmiast reagujemy na większość powiadomień, zwłaszcza tych z komunikatorów. Większość wejść na strony phishingowe

następuje w ciągu 15 minut od otrzymania wiadomości. Najczęściej w takiej sytuacji nie zwracamy uwagi na to, kto do nas napisał, tylko zaczynamy od sprawdzenia, „co podesłał". Jednocześnie koszt wysłania wiadomości phishingowej jest znikomy – to ok. kilkunastu groszy. Można więc łatwo policzyć, że do „zwrotu z inwestycji" w postaci wysłania 10 000 wiadomości SMS wystarczy oszukać jedną osobę na 1000–2000 zł. Raporty publikowane przez NBP[36] pokazują, że skala strat finansowych jest znacznie większa.

Zgłoszenia wiadomości SMS

Wykorzystywaniu SMS-ów do dystrybucji oszustw przyglądamy się bliżej od przełomu 2020 i 2021 roku. Jednym z narzędzi służących do kontroli tego zjawiska są prowadzone przez nas statystyki, które prezentujemy i opisujemy w raportach rocznych. W kwietniu 2021 roku rozpoczęliśmy przyjmowanie zgłoszeń podejrzanych wiadomości za pośrednictwem kanału zgłoszeniowego. Aby uprościć proces zgłaszania, w listopadzie 2023 roku uruchomiliśmy darmowy numer 8080. Było to możliwe dzięki współpracy z rynkiem telekomunikacyjnym oraz za sprawą wejścia w życie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej[37].

Do tej pory co roku notowaliśmy rekordy liczby zgłoszeń SMS, jednak 2025 rok przyniósł załamanie trendu wzrostowego. Przyjęliśmy 295 169 zgłoszeń podejrzanych wiadomości SMS, co stanowi spadek o 16,8% względem roku poprzedniego (354 566). Jeszcze ciekawiej przedstawia się sytuacja związana z wiadomościami sklasyfikowanymi jako złośliwe. W 2024 roku było ich 140 659, a w 2025 roku wartość ta (81 395) spadła do poziomu porównywalnego z 2022 rokiem (82 319). Ciekawie również wygląda porównanie ostatnich kwartałów minionych lat. Dotychczas wzrastała wówczas liczba oszustw związanych z motywem niedostarczenia przesyłki wykorzystujących okres świątecznych zakupów. W latach 2022–2024 złośliwe wiadomości stanowiły średnio 35,4% wszystkich zgłoszeń z czwartego kwartału, natomiast w 2025 roku ten odsetek wyniósł jedynie 10,3%. Wynika to z wystąpienia czynników, które opisujemy poniżej.

Blokowanie złośliwych SMS-ów

Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej powstała m.in. po to, aby dać instytucjom państwowym narzędzia do walki z tego rodzaju zagrożeniami. Jednym z takich narzędzi jest mechanizm blokowania wiadomości SMS.

36 https://nbp.pl/system-platniczy/dane-i-analizy/transakcje-oszukancze

37 https://orka.sejm.gov.pl/proc9.nsf/ustawy/3069_u.htm

Na podstawie analizy otrzymywanych zgłoszeń upubliczniamy wyrażenia regularne, które opisują konkretne wiadomości lub całe kampanie SMS. Rejestr jest aktualizowany za pośrednictwem systemu, do którego dostęp mają operatorzy SMS. W ciągu 5 minut od upublicznienia wzorzec zostaje automatycznie pobrany i operator ma obowiązek blokowania każdej wiadomości, która pasuje do tego wzorca. W ramach walki ze smishingiem prowadzimy również wykaz nadpisów SMS zarezerwowanych dla podmiotów publicznych. Instytucja, która zgłosi taki nadpis, uzyskuje do niego pełne prawo, co skutkuje zablokowaniem próby wysłania wiadomości z danym nadpisem przez innego nadawcę. 2025 był pierwszym rokiem, w którym operatorzy telekomunikacyjni blokowali wiadomości przez okres od stycznia do grudnia. Na podstawie przedstawionych wcześniej statystyk dotyczących liczby samych zgłoszeń możemy stwierdzić, że system blokad może mieć wpływ na wykorzystanie SMS-ów do dystrybucji oszustw.

W 2024 roku wytworzyliśmy 746 wzorców, które przełożyły się na 1 475 678 blokad[38]. W 2025 roku 790 wzorców doprowadziło do zablokowania 1 883 610 złośliwych SMS-ów. Ta statystyka ukazuje rosnącą skuteczność systemu – pierwszy rok jego działania przyniósł średnio 1978 zablokowanych prób oszustwa na jeden wzorzec, w minionym roku były to już 2384 udaremnione próby.

Kluczowy w przeciwdziałaniu oszustwom jest czas reakcji. Zlecenia wysłania kilku czy kilkunastu tysięcy wiadomości trwają zazwyczaj do 30–40 minut. Z tego powodu 10 wzorców może doprowadzić do mniejszej liczby blokad niż pojedynczy, stworzony po otrzymaniu zaledwie kilku zgłoszeń. Dlatego też cały czas rozwijamy nasz system analityczny: w 2024 roku każda zgłoszona złośliwa wiadomość przełożyła się średnio na 24 blokady. W 2025 roku udało nam się utrzymać ten współczynnik na poziomie 23 niedostarczonych wiadomości. Ponownie rekordowym miesiącem okazał się listopad – 84 blokady na każde zgłoszenie smishingu.

Kampanie SMS

W 2025 roku obserwowaliśmy postępującą zmianę w scenariuszach oszustw wykorzystujących SMS-y. Przytoczone wcześniej statystyki sugerowały już, że zmniejszyła się popularność historii związanych z paczkami. Dotyczy to całej grupy wiadomości zawierających link do strony phishingowej. Natomiast odnotowujemy coraz większy odsetek oszustw, w których SMS jest jedynie zachętą lub przynętą do nawiązania kontaktu. Taki motyw pojawia się np. w rzekomych wiadomościach od dziecka o uszkodzeniu telefonu lub karty

38 Dane o zablokowanych wiadomościach SMS są szacowane na podstawie raportów przesyłanych przez operatorów telekomunikacyjnych z uwzględnieniem procentowego udziału tych operatorów w rynku telefonii mobilnej.

SIM i potrzebie kontaktu poprzez inny komunikator, w fałszywych SMS-ach zawierających informacje o zyskach na naszym koncie walutowym/inwestycyjnym lub powiadomienie o próbie logowania na nasze konto kryptowalutowe.

Część tych zmian możemy przypisać mechanizmowi blokowania podejrzanych SMS-ów – zdecydowanie łatwiej nam rozpoznawać smishing zawierający link dzięki analizie pod kątem umieszczenia adresu strony na Liście Ostrzeżeń. Dzięki temu wzorce blokujące wiadomości wysyłane z linkiem powstają trochę szybciej. Innym powodem jest to, że oszuści bardzo szybko dostosowują się do bieżących trendów. Przykładem jest wykorzystanie boomu na inwestycje w ostatnich latach. Przestępcy dobierają odpowiednie scenariusze, aby zwiększyć szanse, że adresat będzie miał znany sobie punkt odniesienia do wiadomości, którą otrzymuje. W znacznej większości nie są to spersonalizowane oszustwa, na korzyść przestępców działa tu efekt skali. Dlatego zawsze warto zadać sobie pytanie, czy paczka, na którą czekamy, na pewno jest dostarczana przez piszącą do nas firmę kurierską, z jakiego powodu doradca lub giełda pisze SMS zamiast wysłać powiadomienie w aplikacji albo czemu nasze dziecko nie poprosiło nauczyciela o poinformowanie nas o zdarzeniu, albo czy w ogóle mamy dziecko.

Niezmiennie zachęcamy do pomocy w walce ze smishingiem poprzez wysyłanie wiadomości pod numer 8080. Jest to nie tylko sposób na uzyskanie odpowiedzi na pytanie „Czy wiadomość jest złośliwa?”, lecz także na ochronę innych użytkowników. W tym procesie to czas reakcji ma największe znaczenie, dlatego prosimy bez wahania zgłaszać podejrzane materiały.

Skoordynowane ujawnianie podatności

W roku 2025 CERT Polska osiągnął znaczące wyniki w obszarze skoordynowanego ujawniania podatności. Opublikowaliśmy 165 identyfikatorów CVE, z czego 8 podatności zostało odkrytych w wyniku badań własnych. Działalność w tym obszarze jest ważnym filarem operacyjnym zespołu w kontekście wdrażania wymogów europejskiego prawodawstwa, szczególnie dyrektywy NIS 2 i rozporządzenia CRA, które definiują nowe obowiązki dla podmiotów uczestniczących w ekosystemie zarządzania podatnościami.

Działalność jako CNA

Od sierpnia 2023 roku CERT Polska ma status CNA (CVE Numbering Authority) i wciąż jest jedynym podmiotem w Polsce uprawnionym do przyznawania identyfikatorów w programie CVE (Common Vulnerabilities

and Exposures), będącym globalnym standardem numerowania i katalogowania podatności w oprogramowaniu. W pierwszym roku operacyjnym (sierpień 2023 – lipiec 2024) CERT Polska opublikował 73 identyfikatory CVE. Systematycznie zwiększamy nasze doświadczenie, zyskujemy zaufanie badaczy bezpieczeństwa i umacniamy kontakty z producentami oprogramowania, co pozwala na efektywniejsze obsługiwanie kolejnych podatności zgłaszanych nam do skoordynowanego ujawnienia.

Rok 2025 przyniósł znaczący wzrost aktywności: łącznie 165 identyfikatorów CVE opublikowanych przez CERT Polska oznacza podwojenie dotychczasowej pracy i odzwierciedla rosnącą liczbę zgłoszeń podatności pochodzących zarówno od badaczy zewnętrznych, jak i z wyników badań własnych zespołu.

TABELA 3. Opublikowane identyfikatory CVE od stycznia do grudnia 2025 roku

Miesiąc 2025	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	Razem
Liczba opublikowanych identyfikatorów CVE	4	9	11	15	22	3	6	36	16	12	21	10	165
Na podstawie badań własnych CERT Polska	0	0	0	0	0	0	0	0	7	1	0	0	8

Liczba opublikowanych w danym miesiącu informacji o podatnościach jest zmienna, ponieważ zgłoszone przypadki mogą dotyczyć jednego lub wielu błędów w tym samym produkcie. W 2025 roku rekordowy dla nas pod względem liczby był zbiór 17 podatności w CGM CLININET opublikowanych 27 sierpnia 2025 roku. Z tego powodu miesiąc ten zapisał się jako najbardziej aktywny pod względem ujawnionych podatności.

Do najistotniejszych podatności ujawnionych z naszą pomocą należały:

- CVE-2025-7063 oraz 8 innych CVE w oprogramowaniu PAD CMS umożliwiające m.in. zmianę hasła dowolnego użytkownika. W odpowiedzi na zidentyfikowane zagrożenia oraz brak dalszego wsparcia dla produktu Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydał rekomendację zaprzestania korzystania z tego oprogramowania.
- CVE-2025-9313 w oprogramowaniu mMedica firmy Asseco Poland S.A. umożliwiające uzyskanie nieautoryzowanego dostępu do bazy danych.
- CVE-2024-8773 i CVE-2024-8774 w oprogramowaniu SIMPLE.ERP umożliwiające zwiększenie uprawnień użytkownika do administratora bazy danych.
- CVE-2025-10910 w produktach Govee z łącznością sieciową umożliwiające przejęcie kontroli nad urządzeniem.

Proces przeprowadzonych przez nasz zespół badań oprogramowania CMS dla Biuletynów Informacji Publicznej został opisany w osobnym artykule (→ s. 93).

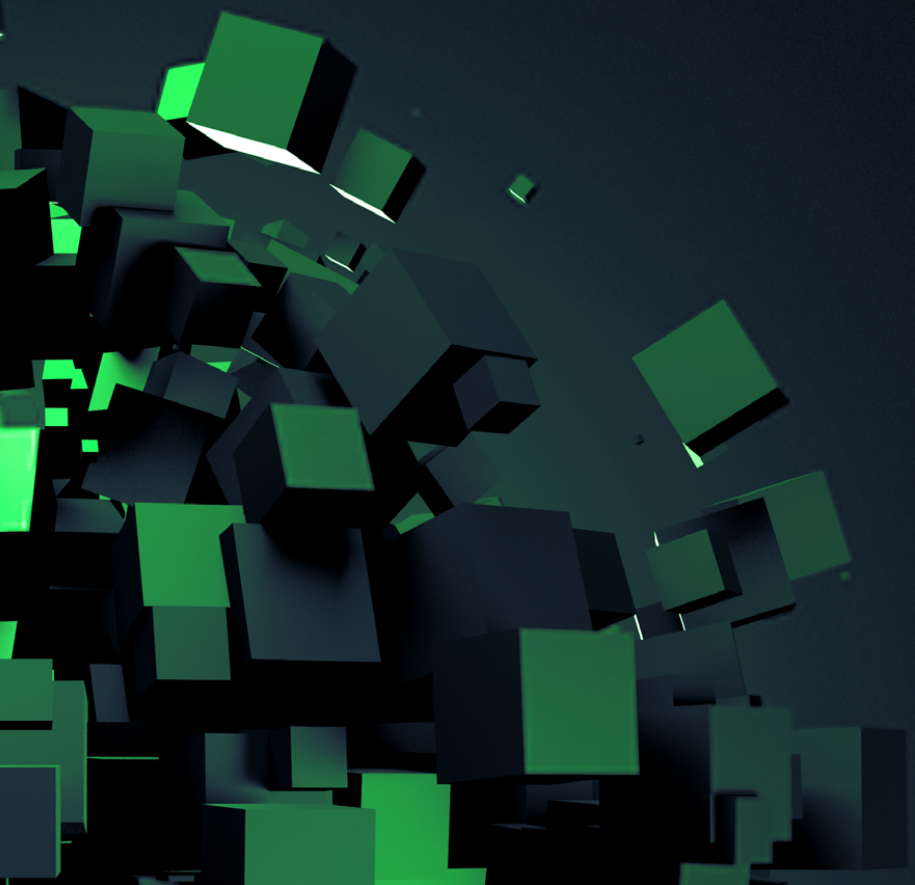
Przykładem skoordynowanego przez nas przypadku ujawnienia podatności, który był szerzej komentowany w środowisku branżowym, jest CVE-2025-4049 w oprogramowaniu FARA firmy SIGNUM-NET. Kontrowersje wzbudziło kwestionowanie przez producenta istnienia i sposobu wykrycia zgłaszanych podatności. Przeprowadzone przez nas kolejne badanie potwierdziło raportowane błędy, co skłoniło producenta do podjęcia działań naprawczych.

Najtrudniejsze z naszej perspektywy są jednak niezmiennie przypadki, gdzie pomimo wielu prób kontaktu z producentem oprogramowania nie otrzymujemy żadnej odpowiedzi, a błędy nie są usuwane. W minionym roku problem ten dotyczył wielu zgłaszanych nieprawidłowości:

- CVE-2025-22270 i 4 innych CVE w oprogramowaniu CyberArk Endpoint Privilege Manager,
- CVE-2024-13892 i 2 innych CVE w kamerach Smartwares CIP-37210AT i C724IP,
- CVE-2025-2098 w oprogramowaniu Fast CAD Reader firmy Beijing Honghu Yuntu Technology,
- CVE-2025-3758 i 1 innego CVE w oprogramowaniu Netis Systems WF2220,
- CVE-2025-53811 w aplikacji Mosh-Pro na systemy operacyjne macOS,
- CVE-2025-7761 w oprogramowaniu Akcess-Net Lepszy BIP,
- CVE-2025-54172 i 14 innych CVE w oprogramowaniu OpenSolution: Quick.CMS, Quick.CMS.Ext, Quick.Cart,
- CVE-2025-9983 w kamerach GALAYOU G2,
- CVE-2025-53701 i 1 innego CVE w kamerach Vilar VS-IPC1002,
- CVE-2025-9977 w oprogramowaniu Times Software E-Payroll,
- CVE-2025-65007 i 4 innych CVE w oprogramowaniu routera WODESYS WD-R608U.

Funkcjonowanie CERT Polska w roli CNA wiąże się ze ścisłym respektowaniem wytycznych międzynarodowego programu CVE. Oznacza to m.in. możliwość obsługi zgłoszeń lub raportowania własnych odkryć jedynie w tych produktach, które nie należą do zakresu odpowiedzialności innych CNA – w takich sytuacjach naszym obowiązkiem jest przekierowanie zgłaszającego do właściwej organizacji. Artykuły zawierające informacje o wszystkich podatnościach ujawnionych przez zespół CERT Polska są publikowane na stronie cert.pl/cve. Więcej informacji o obsłudze zgłoszeń podatności przez nasz zespół znajduje się na stronie cert.pl/cvd.

Statystyki



Zgłoszenia i incydenty

W 2025 roku zespół CERT Polska otrzymał 658 320 zgłoszeń, które zostały szczegółowo przeanalizowane. Na ich podstawie zarejestrowano 260 783 unikalnych incydentów bezpieczeństwa. Są to zdarzenia, które miały lub mogły mieć negatywny wpływ na poziom cyberbezpieczeństwa.

W porównaniu z 2024 rokiem liczba zgłoszeń w 2025 roku wzrosła o 10%, natomiast liczba zarejestrowanych incydentów cyberbezpieczeństwa w 2025 roku zwiększyła się aż o 152% w stosunku do roku poprzedniego. Od wielu lat obserwujemy utrzymującą się tendencję wzrostową liczby rejestrowanych incydentów w skali roku. Wzrost liczby zgłoszeń oraz zarejestrowanych incydentów cyberbezpieczeństwa wynika m.in. z rosnącej świadomości społecznej w zakresie zagrożeń, a także z roli zespołu CERT Polska w monitorowaniu i analizowaniu incydentów cyberbezpieczeństwa oraz reagowaniu na nie. Ważnym czynnikiem wpływającym na świadomość społeczną są prowadzone działania informacyjne dotyczące występujących zagrożeń. W tabeli 5 przedstawiliśmy liczbę incydentów w latach 2018–2025.

Zgłoszenia trafiają do nas poprzez:

- formularz dostępny na stronie https://incydent.cert.pl – zgłoszenie incydentu,
- formularz dostępny na stronie https://incydent.cert.pl/domena – zgłoszenie złośliwej domeny,
- SMS pod numer 8080 – zgłoszenie podejrzanej wiadomości SMS,
- aplikację mObywatel – zgłoszenie złośliwej strony internetowej, oszustwa lub innego zdarzenia (usługa Bezpiecznie w sieci),
- e-mail: cert@cert.pl,
- tradycyjną pocztę na adres NASK–PIB.

Najczęstsze typy incydentów w 2025 roku

Oszustwa komputerowe

Najliczniejszą kategorią incydentów zarejestrowanych w 2025 roku były oszustwa komputerowe. Odnotowano 253 238 takich incydentów, co stanowiło 97% wszystkich obsłużonych zdarzeń. W porównaniu z rokiem poprzednim liczba oszustw komputerowych wzrosła o 158%.

Najczęściej występującym rodzajem oszustw komputerowych były próby wyłudzania poufnych danych, takich jak loginy i hasła do poczty elektronicznej,

serwisów bankowych, portali społecznościowych czy innych usług online (phishing). W 2025 roku odnotowano 78 391 tego typu incydentów, co stanowiło 30% wszystkich zarejestrowanych zdarzeń. Na liście oszustw komputerowych znalazły się m.in. fałszywe sklepy internetowe oraz oszustwa inwestycyjne, w których przestępcy podszywali się pod koncerny paliwowo-energetyczne, firmy, instytucje, wykorzystywali też wizerunki znanych osób. Wśród najczęściej wykorzystywanych kampanii phishingowych znalazły się przypadki nieuprawnionego użycia wizerunku serwisów sprzedażowych OLX – 28 462 zdarzenia, Allegro – 22 513 zdarzeń oraz próby pozyskania poświadczeń do skrzynek elektronicznych – 2519 zdarzeń.

Szkodliwe oprogramowanie

Drugą najczęściej występującą kategorią zagrożeń w 2025 roku było szkodliwe oprogramowanie. Zarejestrowano 3438 incydentów tego typu, które obejmowały m.in. infekcje systemów informatycznych oraz próby nieuprawnionego dostępu z wykorzystaniem szkodliwego kodu. Wśród tych zdarzeń odnotowano 179 przypadków oprogramowania szyfrującego typu ransomware, które mogło prowadzić do utraty dostępności danych lub systemów oraz generować istotne ryzyko dla ciągłości działania podmiotów dotkniętych incydentem. Incydenty związane ze szkodliwym oprogramowaniem nadal stanowią istotne zagrożenie dla bezpieczeństwa teleinformatycznego i wymagają bieżącego monitorowania oraz szybkiego reagowania.

Podatne usługi

Trzecim istotnym rodzajem zagrożeń były podatne usługi. W 2025 roku odnotowano 1732 incydenty tego typu, związane z występowaniem luk bezpieczeństwa w publicznie dostępnych usługach i systemach teleinformatycznych. Incydenty te mogły umożliwiać nieuprawniony dostęp do zasobów, eskalację uprawnień lub zakłócenie działania usług. Zdarzenia związane z podatnymi usługami podkreślają znaczenie regularnych aktualizacji oprogramowania, właściwej konfiguracji systemów oraz bieżącego monitorowania stanu bezpieczeństwa infrastruktury teleinformatycznej.

W tabeli 7 przedstawiliśmy statystyki z podziałem na kategorie incydentów.

Ustawa o krajowym systemie cyberbezpieczeństwa

W 2025 roku CSIRT NASK w ramach ustawy o krajowym systemie cyberbezpieczeństwa obsłużył 27 incydentów zaklasyfikowanych jako poważne. Były to zdarzenia, które spowodowały lub mogły spowodować istotne obniżenie

jakości lub przerwanie ciągłości świadczenia usługi kluczowej. Spośród 27 incydentów poważnych 14 dotyczyło sektora bankowości i infrastruktury rynków finansowych, 8 miało miejsce w sektorze ochrony zdrowia, natomiast 5 było związanych z sektorem transportu. W porównaniu z rokiem 2024 liczba incydentów poważnych w 2025 roku zmniejszyła się o 53%, zaś liczba incydentów poważnych z sektora bankowości i infrastruktury rynków finansowych o 68%. Spadek ten jest związany z wdrożeniem rozporządzenia DORA, które nakłada na podmioty finansowe obowiązek raportowania incydentów poważnych do CSIRT KNF. W 2025 roku nie odnotowano żadnego incydentu istotnego.

W 2025 roku CSIRT NASK obsłużył również 5111 incydentów w podmiotach publicznych, co oznacza wzrost o 48% w porównaniu z rokiem poprzednim.

TABELA 5. Zestawienie liczby incydentów obsłużonych przez CERT Polska w latach 2018–2025

Rok	Liczba incydentów
2025	260 783
2024	103 449
2023	80 267
2022	39 683
2021	29 483
2020	10 420
2019	6484
2018	3739

TABELA 6. Incydenty obsłużone przez CERT Polska w 2025 roku w podziale na sektor gospodarki. Oznaczenie sektorów wg wewnętrznej klasyfikacji CSIRT NASK

Sektor	Liczba incydentów	Procent
Osoby fizyczne	250 595	96,1%
Administracja publiczna	2801	1,1%
Handel hurtowy i detaliczny	2231	0,9%
Inne	1291	0,5%
Oświata i wychowanie	1258	0,5%
Ochrona zdrowia	724	0,3%
Infrastruktura cyfrowa	495	0,2%
Usługi inne	255	0,1%
Kultura i ochrona dziedzictwa narodowego	218	0,1%
Bankowość	179	0,1%
Transport	140	0,1%
Wodociągi	95	0,0%
Produkcja	93	0,0%
Budownictwo i gospodarka nieruchomościami	78	0,0%

Sektor	Liczba incydentów	Procent
Media	60	0,0%
Energetyka	52	0,0%
Logistyka i dystrybucja	36	0,0%
Infrastruktura rynków finansowych	35	0,0%
Gospodarka odpadami	31	0,0%
Rolnictwo	29	0,0%
Hotele, restauracje, catering	23	0,0%
Kultura fizyczna	18	0,0%
Poczta i usługi kurierskie	13	0,0%
Turystyka	10	0,0%
Działalność ubezpieczeniowa	9	0,0%
Wyznania religijne i mniejszości narodowe	5	0,0%
Izby gospodarcze i handlowe	5	0,0%
Rybołówstwo	4	0,0%
Razem	**260 783**	**100,0%**

TABELA 7. Incydenty obsłużone przez CERT Polska w 2025 roku w podziale na kategorie

Kategoria zagrożenia	Liczba incydentów	Procent
Oszustwa komputerowe	253 238	97,1%
Złośliwe oprogramowanie	3438	1,3%
Podatne usługi	1732	0,7%
Obraźliwe i nielegalne treści	950	0,4%
Włamania	750	0,3%
Dostępność zasobów	427	0,2%
Próby włamań	139	0,1%
Atak na bezpieczeństwo informacji	76	0,0%
Inne	18	0,0%
Gromadzenie informacji	15	0,0%
Razem	**260 783**	**100,0%**

MWDB

MWDB to zaawansowana platforma analityczna stworzona przez CERT Polska, służąca do zbierania, analizowania i udostępniania informacji o złośliwym oprogramowaniu. System, który stale rozwijamy, wspiera pracę analityków cyberbezpieczeństwa w Polsce i na świecie, umożliwia bowiem wymianę wiedzy oraz efektywne śledzenie trendów w obszarze szkodliwego oprogramowania. Kod platformy jest udostępniony nieodpłatnie na licencji open source (https://github.com/CERT-Polska/mwdb-core).

Rozwój platformy MWDB

W 2025 roku w ramach platformy MWDB przeanalizowaliśmy ponad 4,1 mln unikalnych próbek złośliwego oprogramowania. Efektem tych analiz było uzyskanie ponad 20,9 tys. nowych unikalnych konfiguracji malware (np. adresów serwerów zarządzających albo kluczy używanych do szyfrowania).

Równolegle z rozwojem bazy danych prowadziliśmy intensywne prace nad samym oprogramowaniem platformy. W 2025 roku opublikowaliśmy 4 nowe wersje MWDB[49], w których zaimplementowaliśmy istotne poprawki wydajnościowe. Część wprowadzonych zmian była efektem współpracy z zewnętrznymi kontrybutorami, co potwierdza aktywne zaangażowanie społeczności w rozwój projektu.

Dynamiczna analiza złośliwego oprogramowania – DRAKVUF Sandbox

Jednym z kluczowych komponentów ekosystemu MWDB jest projekt DRAKVUF Sandbox, wykorzystywany do dynamicznej analizy złośliwego oprogramowania. Mechanizm ten umożliwia bezpieczne uruchamianie podejrzanych plików w izolowanym i ściśle monitorowanym środowisku wirtualnym. Dzięki temu analitycy mogą śledzić rzeczywiste zachowanie próbek, w tym następstwa ich wykonania, takie jak pobranie docelowego złośliwego oprogramowania, próby połączenia się do znanych serwerów Command & Control czy próby kradzieży danych z systemu ofiary. Projekt wykorzystuje do tego celu otwartoźródłowy monitor DRAKVUF autorstwa Tamasa Lengyela (https://github.com/tklengyel/drakvuf), który obserwuje wykonanie próbek z poziomu hipernadzorcy za pomocą mechanizmów introspekcji maszyny wirtualnej (VMI). Pozwala to wykonywać analizy w sposób bezagentowy – bez konieczności instalowania dodatkowego

49 https://github.com/CERT-Polska/mwdb-core/releases

oprogramowania po stronie systemu „gościa”, które mogłoby być wykryte przez analizowany podejrzany program.

Podobnie jak MWDB projekt DRAKVUF Sandbox jest otwarto-źródłowy i jego kod jest dostępny publicznie (https://github.com/CERT-Polska/drakvuf-sandbox).

W 2025 roku projekt przeszedł gruntowną modernizację, która zaowocowała wydaniem wersji v0.19.0 i v0.20.050. Zmiany umożliwiły analizę próbek za pomocą najnowszej wersji silnika DRAKVUF i tym samym nowszej wersji systemu operacyjnego Microsoft Windows (Windows 10 22H2). Znacząco poprawiliśmy również stabilność analiz oraz jakość generowanych raportów analitycznych. W ramach prac nad DRAKVUF Sandbox wprowadziliśmy również istotne poprawki do silnika DRAKVUF.

Użytkownicy platformy MWDB

Platforma MWDB cieszy się rosnącym zainteresowaniem środowiska specjalistów od cyberbezpieczeństwa. W 2025 roku dostęp do platformy otrzymało 696 zewnętrznych użytkowników, a łączna liczba zarejestrowanych zewnętrznych kont w platformie wyniosła 2533.

Moje.cert.pl

Do końca 2025 roku w serwisie moje.cert.pl zarejestrowało się 15 156 użytkowników i dodało 18 315 domen. Serwis realnie wpływa na bezpieczeństwo polskiej cyberprzestrzeni – w 2025 roku w domenach dodanych w serwisie wykryliśmy 531 206 podatności, z czego 21 258 stanowiło wysokie ryzyko. Poinformowaliśmy użytkowników również o 3 914 212 wyciekach haseł, a także o 191 342 zdarzeniach sieciowych, takich jak np. serwery prowadzące skanowanie czy hostujące phishing. Dodatkowo w serwisie opublikowano 70 komunikatów – są one dostępne bez logowania w portalu, ale użytkownicy mogą również zgłosić chęć ich otrzymywania drogą mailową. Do końca 2025 roku z tej możliwości skorzystało 5127 osób.

Więcej na temat portalu można przeczytać w rozdziale „Moje.cert.pl” (s. 106–107).

50 https://github.com/CERT-Polska/drakvuf-sandbox/releases

Artemis

Od początku stycznia do końca grudnia 2025 roku w ramach projektu Artemis przeskanowano łącznie 92 183 domeny i adresy IP oraz 808 331 subdomen.

Skanowano m.in. instytucje wymienione w tabeli poniżej.

TABELA 8. Liczba przeskanowanych domen, subdomen i adresów IP w 2025 roku w podziale na kategorie

Kategoria	Liczba przeskanowanych domen i adresów IP	Liczba przeskanowanych subdomen
Szkoły i placówki oświatowe, m.in. strony szkół podstawowych, ponadpodstawowych oraz policealnych, domeny młodzieżowych domów kultury, przedszkoli czy poradni psychologiczno-pedagogicznych	46 018	400 994
Jednostki samorządu terytorialnego: strony gmin, powiatów, ale także np. strony spółek odpowiedzialnych za wywóz śmieci, archiwalne domeny czy systemy obsługujące pocztę	20 612	157 765
Uczelnie, np. strony uczelni, wydziałów, ale też domeny związane z konferencjami czy projektami naukowymi	7412	85 890
Instytucje kultury, np. strony teatrów, galerii czy bibliotek	6893	36 023
Zgłoszone domeny: domeny firm i instytucji, które zgłosiły je dobrowolnie do skanowania przed uruchomieniem portalu moje.cert.pl	6409	40 180
Sektor zdrowia, m.in. strony szpitali, ale też instytucji publicznych związanych ze zdrowiem	2829	17 422
Gazety i portale informacyjne	2310	84 688
Domeny .gov.pl	1789	28 390
Banki	1125	1625
Operatorzy usług kluczowych	601	17 123
Politycy i partie: strony m.in. kandydatów, posłów, senatorów i partii politycznych w kontekście wyborów np. samorządowych czy prezydenckich	591	16 998

Kategoria	Liczba przeskanowanych domen i adresów IP	Liczba przeskanowanych subdomen
Samorządy zawodowe, np. strony izb lekarskich czy adwokackich	411	3971
Domeny zgłoszone przez Ministerstwo Infrastruktury	338	477
Producenci automatyki przemysłowej	172	5576
Inne	316	12 663

W niektórych przypadkach dana domena może należeć do kilku kategorii.

Domeny z prefiksem www zostały wyłączone z powyższego zestawienia. Oznacza to, że jeśli dana strona jest dostępna zarówno pod adresem www.strona.pl, jak i strona.pl, to zostanie ona uwzględniona raz.

W 2025 roku łącznie zgłoszono 374 068 podatności lub błędnych konfiguracji, w tym 13 629 wiążących się z wysokim, 248 195 – średnim i 112 244 – niskim zagrożeniem. Stanowi to ok. 20-procentowy wzrost względem liczby podatności i błędnych konfiguracji wykrytych w 2024 roku.

Rodzaje znalezionych podatności lub błędnych konfiguracji zebraliśmy w poniższej tabeli. Skanowanie jest automatyczne, dlatego też podane liczby mogą zawierać duplikaty lub odnosić się do sytuacji, w których w rzeczywistości podatność nie występuje, ponieważ np. wykryto niepoprawnie skonfigurowane SSL/TLS w domenie, która w praktyce nie jest używana.

TABELA 9. Liczba znalezionych podatności lub błędnych konfiguracji w 2025 roku i opis ryzyka z nimi związanego

Liczba wystąpień	Rodzaj podatności/ błędnej konfiguracji	Ryzyko związane z podatnością/ błędną konfiguracją
183 700	Korzystanie z nieaktualnego oprogramowania	Atak przy użyciu znanych podatności – niektóre z podatności mogą skutkować tym, że ze strony można pobrać dane, inne pozwalają zmieniać treść strony lub np. uzyskać uprawnienia administratora
58 170	Problemy z konfiguracją SSL/TLS lub podobnych mechanizmów	Przechwycenie komunikacji użytkownika ze stroną – jeżeli dane zostaną przechwycone i przestępca posiada login i hasło, to może on zalogować się do serwisu jako uprawniony użytkownik

Liczba wystąpień	Rodzaj podatności/ błędnej konfiguracji	Ryzyko związane z podatnością/ błędną konfiguracją
51 554	Błędnie skonfigurowane mechanizmy weryfikacji nadawcy poczty e-mail	Wysyłanie fałszywych e-maili – przestępca może podszywać się pod nadawcę z danej domeny
36 264	Przypadki, gdy zasób taki jak np. panel administracyjny czy panel logowania, np. do bazy danych czy usługi zdalnego pulpitu, był dostępny publicznie	Atak jest możliwy np. jeśli jedno z kont ma słabe hasło albo jeśli w usłudze występują podatności
25 684	Przypadki, gdy informacje o konfiguracji serwera, lista subdomen lub listy plików w folderach na serwerze były dostępne publicznie	Może to ułatwić atakującemu rekonesans, poznanie używanego oprogramowania lub nazw plików, które nie powinny być dostępne publicznie, a w konsekwencji także umożliwić ich pobranie
9116	Konkretne krytyczne lub poważne podatności	Na przykład przejęcie strony lub pobranie danych z bazy danych
7468	Przypadki, gdy wrażliwe dane, takie jak kopie zapasowe, kod źródłowy, zrzuty bazy danych czy dziennik zdarzeń serwera były dostępne publicznie	Pobranie wrażliwych danych
1677	Pozostałe podatności o średnim poziomie ryzyka	Na przykład Open Redirect: atakujący może spreparować w domenie podmiotu link, który przekierowuje do dowolnej innej strony, w tym np. zawierającej szkodliwe oprogramowanie
357	Serwery nadal hostujące domeny, które już nie istnieją	Atakujący może komunikować się bezpośrednio z serwerem i wchodzić w interakcje ze stroną, pomimo że jest ona uznawana za usuniętą
78	Przypadki, gdy domena zbliżała się do wygaśnięcia	Niedostępność usługi lub przejęcie domeny przez atakującego

Więcej informacji na temat projektu Artemis można przeczytać w innej części raportu (→ s. 107–109).

Bezpieczna poczta

Wysyłanie fałszywych wiadomości e-mail to technika, z której regularnie korzystają cyberprzestępcy. W związku z tym w 2023 roku stworzyliśmy serwis bezpiecznapoczta.cert.pl. Dzięki niemu organizacje mogą sprawdzać poprawność konfiguracji mechanizmów takich jak SPF, DMARC czy DKIM, które utrudniają podszycie się pod nadawcę z danej