Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

06/2026

SPIS TREŚCI

Rosyjski ekosystem cyberzagrożeń pod presją sankcji. Wnioski dla administracji publicznej i operatorów infrastruktury krytycznej

13 lipca 2026 r. Unia Europejska, Wielka Brytania oraz państwa Sojuszu Północnoatlantyckiego opublikowały skoordynowane oświadczenia dotyczące wrogiej aktywności Federacji Rosyjskiej (FR) w cyberprzestrzeni. W centrum uwagi znalazło się 16. Centrum Federalnej Służby Bezpieczeństwa (FSB), któremu przypisano wieloletnie operacje cyberszpiegowskie oraz działania sabotażowe wymierzone w państwa europejskie, ich administrację publiczną oraz infrastrukturę krytyczną.

Komunikaty opublikowane przez UE, NATO, rząd Wielkiej Brytanii oraz Ministerstwo Spraw Zagranicznych RP (komunikat MSZ) wskazują na rosnącą skalę współpracy pomiędzy rosyjskimi służbami specjalnymi, grupami cyberprzestępczymi, środowiskami haktywistycznymi oraz podmiotami prywatnymi realizującymi działania zgodne z interesami państwa rosyjskiego. Taki model funkcjonowania określany jest coraz częściej mianem „rosyjskiego ekosystemu cyfrowego", w którym granice pomiędzy aktorami państwowymi i niepaństwowymi ulegają zatarciu.

Szczególne znaczenie dla Polski ma fakt, że zarówno Unia Europejska, jak i Wielka Brytania publicznie wskazały na odpowiedzialność 16. Centrum FSB za działania sabotażowe przeciwko polskiej infrastrukturze energetycznej. W komunikacie brytyjskim podkreślono, że atak wymierzony w polską sieć energetyczną mógł doprowadzić do pozbawienia dostaw energii nawet około 500 tys. obywateli w okresie zimowym. Choć operacja zakończyła się niepowodzeniem, stanowi ona istotny sygnał ostrzegawczy dotyczący gotowości Rosji do prowadzenia działań wymierzonych w infrastrukturę krytyczną państw europejskich.

Według stanowiska UE aktywność FSB obejmowała nie tylko Polskę, ale również Francję, Niemcy, Austrię, Finlandię, Holandię, Rumunię, Słowację i Cypr. Ataki były kierowane przeciwko instytucjom rządowym, podmiotom sektora obronnego, przedsiębiorstwom technologicznym oraz organizacjom związanym z badaniami i rozwojem. W przypadku Francji wskazano na działania szpiegowskie prowadzone przeciwko instytucjom państwowym już od 2010 r., natomiast w Polsce odnotowano operacje sabotażowe wymierzone w obiekty infrastruktury energetycznej.

Odpowiedzią społeczności międzynarodowej stał się pakiet sankcji nałożonych przez Unię Europejską i Wielką Brytanię. Obejmują one zarówno funkcjonariuszy rosyjskich służb wywiadowczych, jak i osoby oraz podmioty wspierające operacje w cyberprzestrzeni i działania wpływu. Sankcje są istotnym elementem budowania odpowiedzialności w sferze cyfrowej oraz sygnałem, że państwa demokratyczne są gotowe publicznie przypisywać odpowiedzialność za działania prowadzone przez aktorów sponsorowanych przez państwo.

Równolegle opublikowano wspólne ostrzeżenie cyberbezpieczeństwa przygotowane przez CISA, NSA, FBI oraz służby cyberbezpieczeństwa kilkunastu państw sojuszniczych, w tym Polski. Dokument opisuje sposób działania grup powiązanych z FSB Center 16, które od wielu lat wykorzystują niewłaściwie skonfigurowane urządzenia sieciowe, przede wszystkim routery i elementy infrastruktury teleinformatycznej. Szczególnym celem pozostają sektory energetyczny, administracji publicznej, finansowy, ochrony zdrowia, komunikacji oraz przemysłu obronnego.

Analiza wskazuje, że znacząca część skutecznych ataków nie wymaga wykorzystywania zaawansowanych podatności typu „zero-day". Atakujący często korzystają z błędów konfiguracyjnych, przestarzałych protokołów zarządzania oraz urządzeń, które nie są odpowiednio aktualizowane. Eksperci rekomendują m.in. wdrażanie nowoczesnych mechanizmów uwierzytelniania, ograniczenie dostępu do interfejsów administracyjnych, wyłączenie nieużywanych usług sieciowych, regularne aktualizowanie oprogramowania oraz ciągłe monitorowanie ruchu sieciowego.

Z perspektywy polskiej administracji publicznej i operatorów usług kluczowych najważniejszym wnioskiem jest konieczność traktowania cyberbezpieczeństwa jako integralnego elementu bezpieczeństwa państwa. Współczesne operacje w cyberprzestrzeni nie służą wyłącznie pozyskiwaniu informacji. Coraz częściej ich celem jest zakłócanie funkcjonowania usług publicznych, destabilizacja gospodarcza, wywieranie presji politycznej oraz wpływanie na procesy decyzyjne państw demokratycznych.

W opublikowanym 13 lipca komunikacie Ministerstwo Spraw Zagranicznych RP podkreśliło pełne poparcie dla działań UE i NATO, wskazując jednocześnie na konieczność dalszego wzmacniania odporności państwa, ochrony infrastruktury krytycznej oraz rozwijania zdolności cyberobronnych. W obliczu stale rosnącego poziomu zagrożeń działania te powinny pozostać jednym z priorytetów krajowego systemu cyberbezpieczeństwa.

Opisywane wydarzenia pokazują, że cyberprzestrzeń stała się jednym z kluczowych obszarów rywalizacji geopolitycznej. Skuteczna ochrona zasobów państwa wymaga nie tylko inwestycji technologicznych, ale również ścisłej współpracy administracji publicznej, operatorów infrastruktury krytycznej, sektora prywatnego oraz partnerów międzynarodowych. Wspólne działania podjęte przez UE, NATO i państwa sojusznicze potwierdzają, że odporność cyfrowa jest dziś jednym z fundamentów bezpieczeństwa narodowego i europejskiego.

Źródło: consilium.europa.eu, nato.int, gov.uk, cisa.gov, cert.pl, gov.pl

Strategiczny projekt cyberbezpieczeństwa z zielonym światłem do dalszych prac

19 czerwca 2026 r. projekt „Wsparcie realizacji zadań Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC)" został umieszczony na „Liście projektów przewidzianych do wyboru w sposób niekonkurencyjny w programie Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC)".

Oznacza to ważny krok w kierunku uruchomienia przedsięwzięcia, którego celem jest dalsze wzmacnianie krajowego systemu cyberbezpieczeństwa oraz rozwój narzędzi służących ochronie administracji publicznej, infrastruktury krytycznej i obywateli przed rosnącą liczbą zagrożeń w cyberprzestrzeni.

Kluczowy projekt dla bezpieczeństwa cyfrowego państwa

Projekt „Wsparcie realizacji zadań PCOC będzie realizowany przez Ministra Cyfryzacji (MC) we współpracy z NASK PIB. Całkowita wartość projektu to 230 mln zł, z czego ponad 206 mln zł stanowić będzie dofinansowanie ze środków UEj w ramach programu FERC.

Celem projektu jest zwiększenie poziomu cyberbezpieczeństwa państwa poprzez rozwój zdolności operacyjnych, analitycznych i koordynacyjnych instytucji odpowiedzialnych za cyberbezpieczeństwo na poziomie krajowym. Projekt wpisuje się w działanie FERC.04.01 *„Wzmocnienie cyberbezpieczeństwa oraz rozwój odpornej infrastruktury przetwarzania danych"*.

Wśród najważniejszych działań przewidzianych do realizacji znajdują się:

- wsparcie funkcjonowania PCOC,
- rozwój krajowych zdolności analitycznych i wymiany informacji o zagrożeniach,
- wdrożenie platform Cyber Threat Intelligence (CTI),
- rozbudowa systemu ochrony przed atakami DDoS dla podmiotów publicznych i kluczowych dla bezpieczeństwa państwa,
- dalszy rozwój systemu S46, wspierającego obsługę incydentów cyberbezpieczeństwa,
- rozbudowa portalu cyber.gov.pl jako centralnego punktu dostępu do usług i informacji z zakresu cyberbezpieczeństwa.

Projekt ma charakter ogólnokrajowy.

Umieszczenie projektu na liście projektów przewidzianych do wyboru w sposób niekonkurencyjny nie oznacza jeszcze automatycznego przyznania dofinansowania. Kolejnym etapem będzie przygotowanie i złożenie wniosku o dofinansowanie, a następnie przeprowadzenie oceny projektu przez właściwą instytucję zarządzającą programem FERC. Dopiero pozytywna ocena oraz zawarcie umowy lub porozumienia o dofinansowanie umożliwią rozpoczęcie finansowania przedsięwzięcia ze środków europejskich.

Realizacja projektu planowana jest na lata 2026 – 2030, a jego efektem ma być zwiększenie odporności krajowego systemu cyberbezpieczeństwa, skuteczniejsze reagowanie na incydenty oraz zapewnienie bezpiecznych i niezawodnych usług cyfrowych dla administracji, przedsiębiorców i obywateli.

1. Korzyści dla obywateli, administracji i podmiotów kluczowych

Realizacja projektu przyniesie wymierne korzyści zarówno obywatelom, jak i instytucjom publicznym oraz podmiotom kluczowym funkcjonującym w ramach krajowego systemu cyberbezpieczeństwa.

2. Korzyści dla obywateli

Dzięki rozwojowi centralnych systemów cyberbezpieczeństwa oraz zwiększeniu zdolności państwa do wykrywania i neutralizowania zagrożeń cyfrowych, obywatele będą mogli korzystać z bezpieczniejszych i bardziej niezawodnych usług publicznych świadczonych drogą elektroniczną. Ograniczone zostanie ryzyko zakłóceń w działaniu kluczowych e-usług administracji, a także wycieków danych i skutków cyberataków wymierzonych w instytucje publiczne. Ważnym elementem projektu będzie również dalszy rozwój portalu cyber.gov.pl, który zapewni dostęp do informacji, ostrzeżeń i usług związanych z cyberbezpieczeństwem w jednym miejscu.

3. Korzyści dla podmiotów kluczowych i ważnych

Projekt wesprze podmioty kluczowe i ważne, które zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa odpowiadają za świadczenie usług niezbędnych dla funkcjonowania państwa i gospodarki. Rozwój systemu S46 usprawni wymianę informacji o incydentach oraz proces zarządzania zagrożeniami, natomiast wdrożenie platform CTI pozwoli na szybsze identyfikowanie nowych zagrożeń i podatności. Rozbudowany system AntyDDoS zapewni skuteczniejszą ochronę przed atakami mogącymi zakłócić funkcjonowanie usług kluczowych dla obywateli i przedsiębiorców.

4. Korzyści dla administracji publicznej

Projekt przyczyni się do zwiększenia zdolności operacyjnych administracji publicznej w zakresie monitorowania, analizy i reagowania na incydenty cyberbezpieczeństwa. Usprawniona zostanie współpraca pomiędzy instytucjami odpowiedzialnymi za bezpieczeństwo państwa, w tym MC, CSIRT-ami poziomu krajowego oraz innymi podmiotami uczestniczącymi w działaniach PCOC. Pozwoli to na szybsze podejmowanie decyzji i skuteczniejszą koordynację działań podczas poważnych incydentów cyberbezpieczeństwa.

5. Korzyści dla państwa i gospodarki

Projekt przyczyni się do zwiększenia odporności krajowego systemu cyberbezpieczeństwa na cyberataki, awarie i sytuacje kryzysowe. Wzmocnione zostaną mechanizmy ochrony infrastruktury cyfrowej oraz zdolności państwa do przeciwdziałania zagrożeniom o charakterze transgranicznym. Długofalowym efektem będzie wzrost zaufania do usług cyfrowych, poprawa bezpieczeństwa przetwarzanych danych oraz zapewnienie ciągłości działania kluczowych usług publicznych i gospodarczych. Projekt będzie również wspierał realizację celów Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej oraz dalszą cyfryzację państwa.

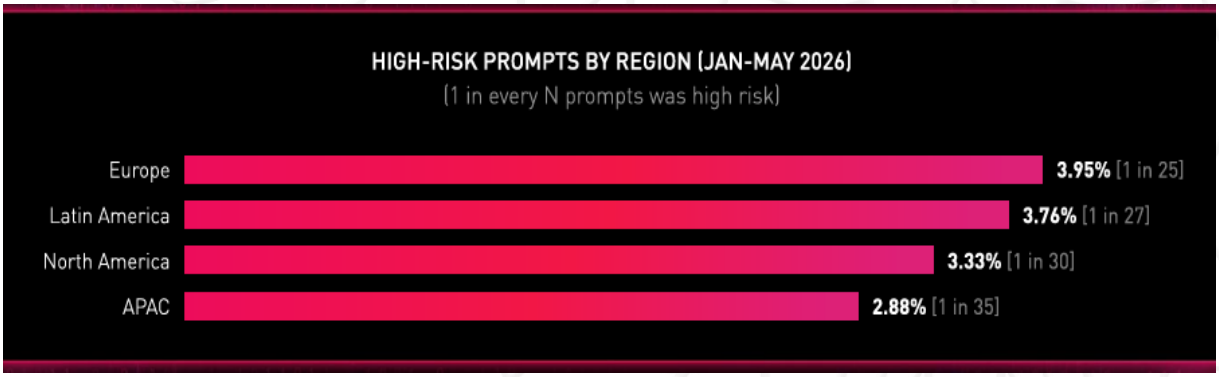
W efekcie projekt będzie oddziaływał nie tylko na instytucje bezpośrednio zaangażowane w jego realizację, lecz również na tysiące podmiotów krajowego systemu cyberbezpieczeństwa oraz miliony obywateli korzystających każdego dnia z usług cyfrowych państwa.

AI jako pole walki w cyberbezpieczeństwie – AI Security Report 2026

W lipcu br. ukazał się raport *AI Security Report 2026* opracowany przez Check Point Research. Raport ten pokazuje, że sztuczna inteligencja przestała być jedynie narzędziem wspomagającym działania człowieka, a coraz częściej staje się samodzielnym uczestnikiem cyberataków – samodzielnym operatorem w łańcuchu ataków.

Bariera eksperckości, która kiedyś istniała zniknęła i obecnie AI wciągu minuty potrafi wykonywać zadania, które kiedyś zajmowały dni. Przykładem może być system VoidLink – profesjonalne narzędzie do ataków, które zostało napisane przez jedną osobę z pomocą ogólnodostępnego AI. Co ciekawe analiza gotowego kodu nie pozwalała stwierdzić, że został on wygenerowany przy pomocy sztucznej inteligencji. Fakt ten ujawniono jedynie dlatego, że twórca popełnił błąd operacyjny i przypadkowo ujawnił swój proces pracy. Pokazuje to, że identyfikacja wykorzystania AI podczas tworzenia złośliwego oprogramowania staje się praktycznie niemożliwa.

Jak Hakerzy oszukują AI? Znaleźli oni sprytne sposoby by zmusić sztuczną inteligencje do łamania swoich własnych zasad. Są to min. Prompt injection – polegające na to na chowaniu złośliwych instrukcji tam, gdzie AI „zagląda" – np. w treści e-maila, na stronie internetowej czy w zaproszeniu w kalendarzu. Gdy AI przeczyta taką wiadomość, może wykonać polecenie hakera, np. wysłać mu twoje hasła. Innym sposobem jest zatruta pamięć, hakerzy potrafią karmić AI fałszywymi informacjami, aż zacznie ona uważać oszustów za zaufane źródło. Kolejnym sposobem jest podrzucanie AI złośliwych plików konfiguracyjnych które AI uznaje za nadrzędne instrukcje. Dzięki temu sztuczna inteligencja automatycznie wyłącza swoje zabezpieczenia przy każdym uruchomieniu



Odsetek interakcji z AI o wysokim ryzyku w podziale na regiony (styczeń–maj 2026 r.)

Raport zwraca również uwagę na zmianę sposobu wykorzystywania sztucznej inteligencji przez przestępców. Początkowo modele AI służyły głównie do generowania tekstów lub prostego kodu, natomiast obecnie potrafią wspierać całe procesy operacyjne. Opisane w raporcie przypadki pokazują, że AI jest zdolna do samodzielnego prowadzenia działań po uzyskaniu dostępu do infrastruktury ofiary – analizuje zebrane dane, proponuje kolejne kroki ataku, a nawet automatycznie wykonuje tysiące poleceń administracyjnych.

Autorzy zwracają również uwagę na wpływ sztucznej inteligencji na proces wyszukiwania podatności w oprogramowaniu. Zaawansowane modele są obecnie zdolne do automatycznej

analizy ogromnych ilości kodu źródłowego oraz wykrywania tysięcy krytycznych luk bezpieczeństwa. Jednocześnie te same możliwości mogą zostać wykorzystane przez cyberprzestępców do błyskawicznego opracowywania exploitów. W rezultacie czas pomiędzy ujawnieniem podatności a jej praktycznym wykorzystaniem systematycznie się skraca, zmuszając organizacje do znacznie szybszego wdrażania aktualizacji bezpieczeństwa

Raport kończy się ważnym przesłaniem skierowanym do osób odpowiedzialnych za bezpieczeństwo organizacji. Tradycyjne metody ochrony sieci komputerowych nie są już wystarczające w środowisku, w którym zarówno atakujący, jak i obrońcy korzystają z zaawansowanej sztucznej inteligencji. Konieczne staje się monitorowanie sposobu wykorzystywania narzędzi AI przez pracowników, kontrolowanie dostępu agentów do danych, zabezpieczanie modeli przed manipulacją oraz wdrażanie polityk bezpieczeństwa dostosowanych do nowych technologii. Jednocześnie AI nie powinna być postrzegana wyłącznie jako źródło zagrożeń – odpowiednio wykorzystana może znacząco wspierać wykrywanie incydentów, analizę podatności oraz automatyzację procesów reagowania na cyberataki.

Warto wspomnieć, że w lipcu 2026 roku NASK dołączył do światowej cyberelity, zyskując jako pierwszy kraj w regionie dostęp do najnowszego modelu GPT-5.5 Cyber od OpenAI. To innowacyjne narzędzie, udostępnione ramach programu Government Trusted Access for Cyber (część inicjatywy Daybreak), pełni rolę cyfrowego „mnożnika siły". Jego głównym celem jest odwrócenie asymetrii sił w sieci na korzyść „obrońców", co pozwala polskim ekspertom na wykrywanie i automatyczne naprawianie podatności z prędkością znacznie przewyższającą możliwości człowieka. W praktyce GPT-5.5 Cyber jest już wykorzystywany do skanowania systemów administracji publicznej oraz infrastruktury krytycznej, analizy złośliwego oprogramowania i zadań z obszaru informatyki śledczej. Model ten potrafi błyskawicznie przeszukiwać ogromne bazy kodu i analizować złożone ścieżki ataków, które wcześniej wymagały tygodni żmudnej pracy specjalistów. Mimo tak ogromnego wsparcia technologicznego, eksperci NASK zaznaczają, że kluczowym ogniwem pozostaje człowiek – to specjaliści NASK weryfikują ostatecznie wyniki analizy przeprowadzonej przez AI, dbając o to, by te nowoczesne narzędzia były wykorzystywane w sposób odpowiedzialny i skuteczny. Dzięki temu Polska zyskała status „zweryfikowanego obrońcy", co stanowi wyraz międzynarodowego zaufania i uznania dla merytorycznej wiedzy naszych rodzimych ekspertów

Ministerstwo Cyfryzacji zapewnia centralnie system rozpoznawania zagrożeń w cyberprzestrzeni (CTI) na potrzeby własne i instytucji zapewaniających cyberbezpieczeństwo na poziomie krajowy. Integralną częścią tego systemu jest moduł AI, zapewnia on wsparcie nawet przy najbardziej żmudnych etapach analizy zagrożeń. Specjaliści mogą po prostu zapytać czy np. adres internetowy jest groźny lub jakie metody stosuje konkretna grupa hakerska. Takie podejście drastycznie skraca czas trwania incydentów pozwala na błyskawiczne podejmowanie decyzji bez konieczności ręcznego przeszukiwania setek artykułów i raportów

Źródło: research.checkpoint.com, nask.pl

Warszawa stanie się stolicą polskiej cyberbezpieczeństwa. Startuje VIII Forum Cyberbezpieczeństwa

Warszawa, 30 września – 1 października 2026 r. Ataki hakerskie na instytucje publiczne, dezinformacja podszywająca się pod prawdziwe źródła, rosnąca presja geopolityczna na infrastrukturę krytyczną - to codzienność, z którą mierzą się dziś eksperci, urzędnicy i przedsiębiorcy. Odpowiedzią na te wyzwania będzie już ósma edycja Forum Cyberbezpieczeństwa, organizowanego przez Ministerstwo Cyfryzacji we współpracy z Miastem Stołecznym Warszawa. Wydarzenie otworzy Miesiąc Cyberbezpieczeństwa.

Przez dwa dni Pałac Kultury i Nauki stanie się miejscem spotkań osób, które na co dzień odpowiadają za bezpieczeństwo polskiej i europejskiej przestrzeni cyfrowej - od decydentów rządowych, przez ekspertów technicznych, po przedstawicieli biznesu i mieszkańców Warszawy. To nie będzie kolejna konferencja pełna ogólników - organizatorzy zapowiadają intensywny program debat, warsztatów i prezentacji skoncentrowanych na tym, co dziś najbardziej istotne: aktualnych trendach w cyberbezpieczeństwie, kierunkach polityk regulacyjnych, współpracy międzynarodowej oraz coraz ważniejszym - partnerstwie sektora publicznego i prywatnego. Nowością będzie „Strefa Warszawiaka", poświęcona cyberhgienie, dezinformacji, wypełniona praktycznymi warsztatami i prelekcjami. Skorzystać z niej będzie mógł każdy wcześniej zarejestrowany uczestnik.

Kolarz zdjęć z roku poprzedniego

Dlaczego to wydarzenie ma znaczenie

Cyberbezpieczeństwo przestało być tematem wyłącznie dla ekspertów. To dziś kwestia bezpieczeństwa narodowego, stabilności gospodarczej i zaufania obywateli do instytucji państwa. Forum Cyberbezpieczeństwa od siedmiu edycji buduje przestrzeń, w której te wątki

się spotykają - a fakt, że tegoroczna odsłona rusza właśnie w Warszawie, przy wsparciu władz miasta, podkreśla rangę stolicy jako centrum polskiej debaty o cyberbezpieczeństwie.

Rozpoczynając Miesiąc Cyberbezpieczeństwa, Forum staje się punktem wyjścia do szerszej, ogólnopolskiej rozmowy - sygnałem, że ochrona danych, systemów i infrastruktury to sprawa wspólna, wymagająca zaangażowania administracji, biznesu i społeczeństwa.

Czego można się spodziewać

Dwa dni wydarzenia to gęsty program, w którym znajdą się m.in.:

- debaty o najnowszych trendach i zagrożeniach w cyberprzestrzeni,
- dyskusje o kierunkach polskich i europejskich polityk cyberbezpieczeństwa,
- rozmowy o współpracy międzynarodowej w reagowaniu na incydenty i budowaniu odporności,
- warsztaty i sesje poświęcone praktycznej współpracy sektora publicznego z prywatnym.
- „strefa Warszawiaka" dla każdego obywatela, poświęcona cyberhigienie, dezinformacji z konkursami i symulacjami cyberataków.

Więcej informacji i rejestracja:

Szczegółowy program, listę prelegentów oraz informacje o rejestracji wkrótce będzie dostępna:

- *na stronie internetowej: https://cyber.gov.pl/forum-cyber*
- *na LinkedIn: https://www.linkedin.com/showcase/forum-cyberbezpiecze%C5%84stwa/*

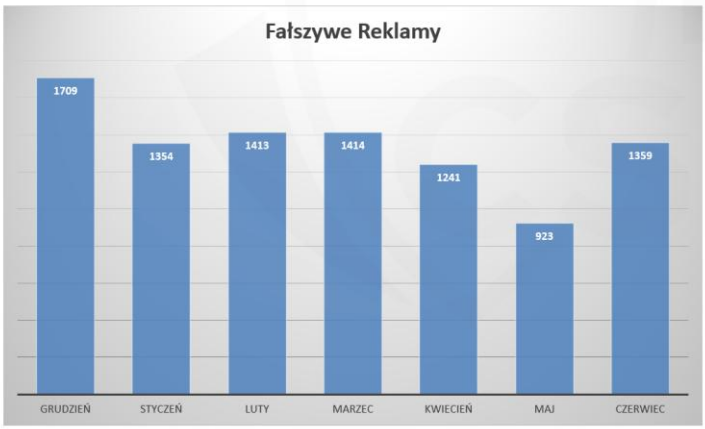
Podsumowanie miesiąca przez CSIRT KNF - Krajobraz zagrożeń skierowanych na klientów rynku finansowego - czerwiec 2026

Zespół CSIRT KNF w minionym miesiącu ponownie zidentyfikował szereg kampanii przestępczych, które miały na celu wyłudzanie danych oraz pieniędzy od klientów sektora bankowego. Choć część schematów pozostaje niezmienna, cyberprzestępcy nieustannie je modyfikują oraz dopasowując narracje do aktualnych trendów i wydarzeń.

Statystyki i działania operacyjne

W czerwcu 2026 roku CSIRT KNF wykrył i zgłosił do zablokowania 1608 domen, które wcześniej zakwalifikowane zostały jako wyłudzające dane (m.in. loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe), dla porównania CERT Polska dodał na listę ostrzeżeń 21 176 domen. A na koniec omawianego miesiąca, na liście hole znajdowało się 126 820 domen.

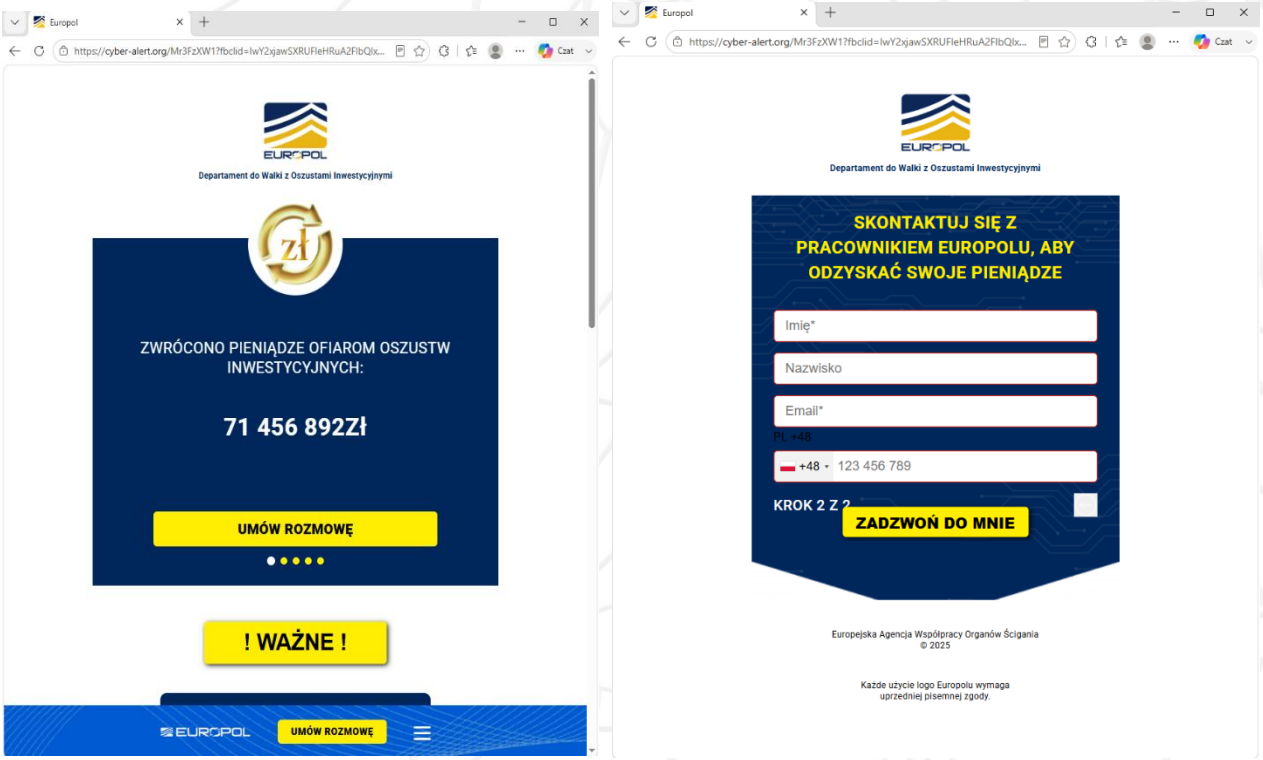
Zdecydowana większość zgłoszonych domen phishingowych wykorzystywana była w scenariuszu znanym pod nazwą „fraud inwestycyjny". Schemat działania przestępców, w którym zachęcają do rzekomego inwestowania, a w rzeczywistości powodujące wysokie straty finansowe u klientów banków. Najczęstszym sposobem dystrybucji tego typu treści są reklamy w mediach społecznościowych. Poniższe wykresy przedstawiają wykryte i zgłoszone do blokady reklamy na portalu społecznościowym Facebook, w podziale na kategorie wykorzystywanego wizerunku.



Przestępcy reklamując rzekome inwestycje wykorzystują często wizerunki znanych osób, wizerunki rozpoznawalnych firm oraz motywy rządowe. Nadal chętnie wykorzystują również technologię deepfake do tworzenia materiałów oszukańczych. Przedstawiona treść zachęca do rzekomych inwestycji.

Rysunek 1.Fałszywe reklamy zamieszczane przez cyberprzestępców na portalu Facebook

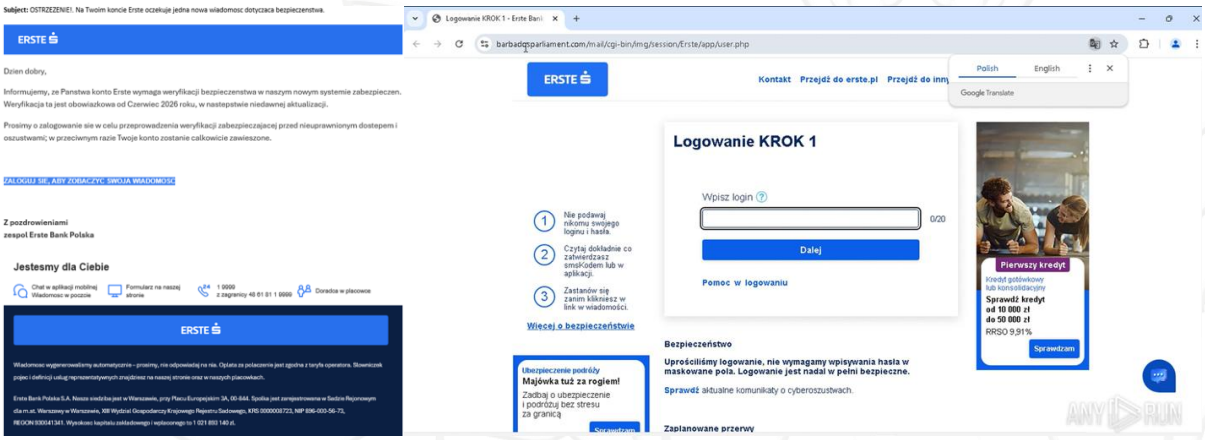
Cyberprzestępcy w ostatnim miesiącu wykorzystywali motyw zwrotu straconych środków. W reklamach publikowanych na Facebooku podszywali się pod Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) i obiecywali pomoc w odzyskaniu pieniędzy. Po kliknięciu reklama prowadziła do fałszywych stron podszywających się pod Europol, gdzie oszuści zachęcali do dokonania rejestracji. W kolejnym kroku cyberprzestępcy kontaktowali się z ofiarami i próbowali nakłonić do wpłacenia kolejnych oszczędności – rzekomo po to, aby „odblokować zwrot" lub „przyśpieszyć procedurę". W rzeczywistości była to próba ponownego oszustwa.



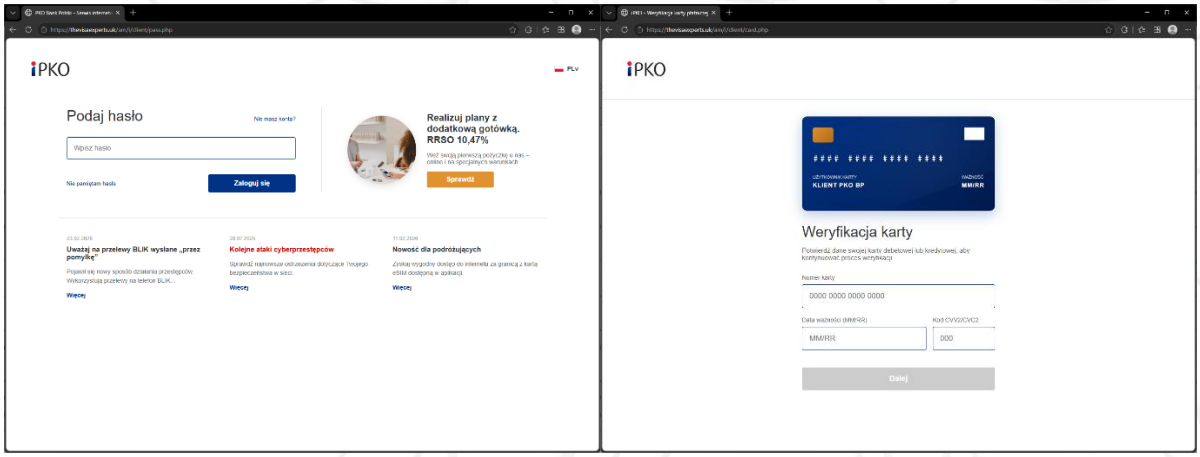
Rysunek 2. Fałszywe inwestycje – formularz rejestracyjny

Przestępcy wykorzystują również wizerunek znanych instytucji, aby zwiększać wiarygodność kampanii phishingowych, dlatego też regularnie podszywają się pod polskie Banki. Wyłudzają w ten sposób m.in informacje o kartach płatniczych, dane uwierzytelniające do bankowości elektronicznej, czy kody BLIK. W czerwcu 2026 roku nadal wykorzystywali ten sposób. Zidentyfikowane kampanie phishingowe wykorzystywały wizerunki m.in:

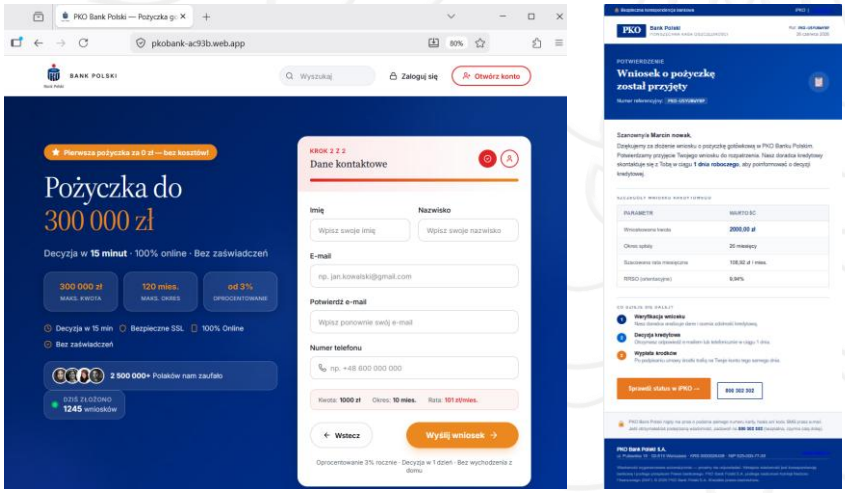
- Erste Bank Polska,



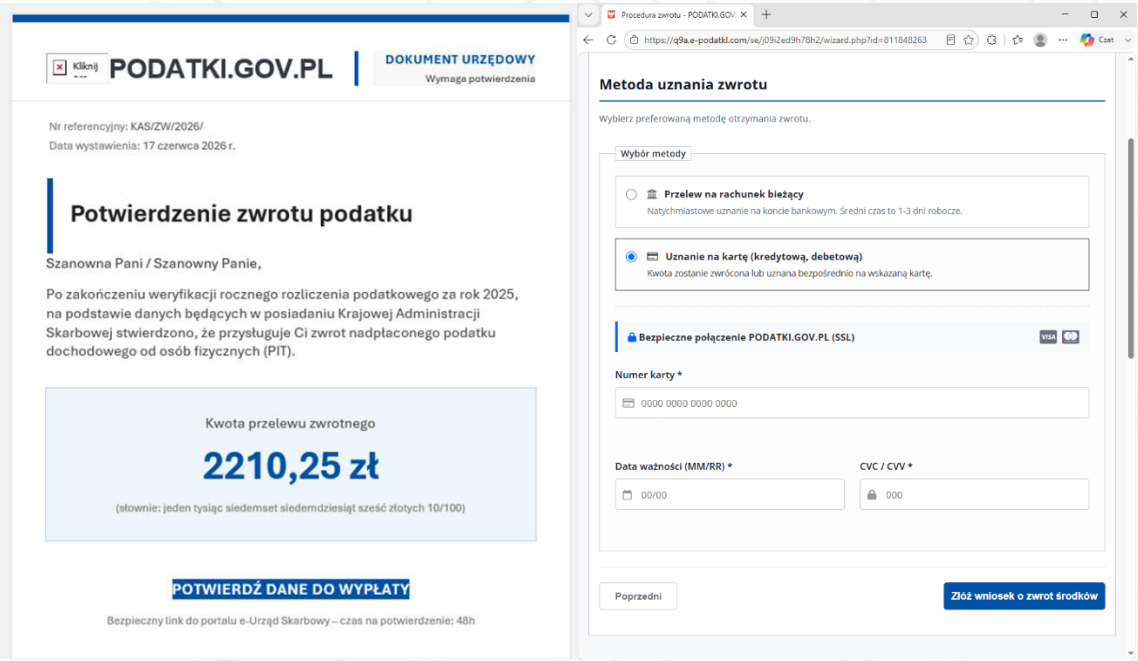
- iPKO,



- PKO BP,



W czerwcu 2026 oszuści przesyłali także fałszywe wiadomości e-mail o rzekomej nadpłacie podatku dochodowego, w których podszywali się pod Krajową Administrację Skarbową (KAS) oraz portal podatki.gov.pl (rys.4). Cyberprzestępcy zachęcali do kliknięcia w link z wiadomości. W rzeczywistości prowadził on na stronę, na której oszuści próbowali wyłudzić numer PESEL, inne dane osobowe oraz informacje o kartach płatniczych. Przykładem kolejnej kampanii, z jaką mieliśmy do czynienia w ostatnich tygodniach było podszycie pod Stalexport Autostrada Małopolska. Cyberprzestępcy przygotowali strony, na których informowali o mandacie i konieczności jego uregulowania. W rzeczywistości była to strona phishingowa wyłudzająca dane kart płatniczych. Cyberprzestępcy podszywając się pod Pocztę Polską, przesyłali także fałszywe wiadomości SMS, w których informowali o rzekomym błędzie w stanie rozliczeń ubezpieczenia zdrowotnego. Oszuści zachęcali do kliknięcia w znajdujący się w wiadomości link, a w kolejnym kroku wymagali podania swojego numeru PESEL oraz informacji o karcie płatniczej.



Rysunek 3 Fałszywa wiadomość e-mail oraz strona phishignowa – podszycie pod KAS oraz portal podatki.gov.pl

Tak jak zaznaczamy co miesiąc, jedną z metod ochrony przed wymienionymi wyżej i innymi działaniami cyberprzestępców jest wiedza. Dlatego zachęcamy do śledzenia informacji o bieżących schematach i scenariuszach przestępczych na naszych profilach w mediach społecznościowych.

Więcej o działalności CSIRT KNF na poniższych stronach internetowych:

BIULETYN INFORMACYJNY MC – ZAGROŻENIA W CYBERPRZESTZRENI

„Biuletyn Informacyjny. Zagrożenia w cyberprzestrzeni" - opracowywany jest przez zespół Departamentu Cyberbezpieczeństwa MC we współpracy z CBZC i CSIRT KNF.

Ideą Biuletynu jest zwiększanie świadomości i wiedzy na szerokorozumiane tematy związane z cyberbezpieczeństwem wśród pracowników administracji publicznej, zarówno na poziomie centralnym jak i na szczeblu samorządowym.

Możliwość dołączenia do subskrypcji Biuletynu pod linkiem:

– https://www.gov.pl/web/baza-wiedzy/subskrypcja

INFORMACJA O SZKOLENIACH

Zachęcamy również do udziału w bezpłatnych szkoleniach online dla podmiotów krajowego systemu cyberbezpieczeństwa, które organizuje Departament Cyberbezpieczeństwa MC.

Wszystkie informacje na temat szkoleń (w tym harmonogram i formularze zgłoszeń) znajdują się na stronie internetowej Bazy Wiedzy cyberbezpieczeństwa na portalu *gov.pl* – pod linkiem:

– https://www.gov.pl/web/baza-wiedzy/szkolenia

BIULETYN NASK

Zachęcamy również do zasubskrybowania biuletynu NASK – jest to przegląd najważniejszych informacji nt. cyberbezpieczeństwa, edukacji cyfrowej i nowych technologii. Link do zapisów:

– https://www.nask.pl/pl/aktualnosci/5166,Subskrybuj-Biuletyn-NASK-na-LinkedIn.html

Oznaczenia TLP

Traffic Light Protocol (TLP) jest to zestaw reguł, pogrupowanych w 4 kategorie, używanych w celu lepszego zdefiniowania grupy odbiorców wrażliwych informacji. Dla ułatwienia kategorie opisywane są czterema kolorami (czerwony, pomarańczowy, zielony oraz biały). Zakwalifikowanie do odpowiedniej kategorii leży po stronie organizacji, z której pochodzą informacje. Jeśli odbiorca chciałby podzielić się uzyskanymi informacjami z szerszym gronem, musi uzyskać odpowiednią akceptację od autora wiadomości.

Oznaczenie	Odbiorca wiadomości	Autor wiadomości
TLP:RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.	Oznaczenie wiadomości, które mogą za sobą nieść poważne zagrożenie ujawnienia wrażliwych danych w wyniku ich nieprawidłowego przetworzenia, jak również, gdy ich wykorzystanie przez innych niż odbiorcy nie ma sensu.
TLP:AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i consituency) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane. Jednym ze standardowych ograniczeń jest oznaczenie **TLP:AMBER+STRICT , które pozwala dzielić się informacjami wyłącznie w obrębie organizacji.**	Oznaczenie wiadomości wymagających podjęcia odpowiednich kroków przez dodatkowe osoby. Informacje te niosą ze sobą ryzyko ujawnienia zbyt wielu wrażliwych danych, jeśli zostałyby przekazane podmiotom innym niż bezpośrednio zaangażowanym.
TLP:GREEN	Odbiorcy mogą dzielić się informacji ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.	Oznaczenie wiadomości niosących ze sobą informacje ogólnie przydatne dla wszystkich organizacji partnerskich oraz w obrębie środowiska.
TLP:CLEAR	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).	Oznaczenie wiadomości, których wykorzystanie nie powinno wiązać się z żadnym bądź minimalnym ryzykiem niewłaściwego użycia.

Źródło: *cert.pl*

Biuletyn został opracowany przez Wydział Analiz Cyberbezpieczeństwa Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji we współpracy z zespołami CSIRT KNF i CBZC.

Więcej o działalności MC na poniższych stronach: