Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

05/2025

SPIS TREŚCI

Dostęp do informacji publicznej a cyberbezpieczeństwo 3

Globalna operacja przeciwko Lumma Stealer 4

„Parasol Wyborczy" - podsumowanie 5

S46 – centralny system wspierający cyberbezpieczeństwo podmiotów objętych KSC .. 6

17 podejrzanych za oszustwa typu Business Email Compromise (BEC) w rękach policjantów CBZC. Na rachunkach bankowych zabezpieczono ponad 21 mln zł 9

Wspólne działania CBZC i KAS - rozbicie grupy przestępczej, która pod przykrywką działalności charytatywnej wyłudziła niemal 15 milionów złotych! 10

Podsumowanie miesiąca przez CSIRT KNF – Ochrona klienta 11

INFORMACJA O SZKOLENIACH 14

BIULETYN NASK 14

Oznaczenia TLP 15

Dostęp do informacji publicznej a cyberbezpieczeństwo

Na podstawie ustawy o dostępie do informacji publicznej każdy może zawnioskować do podmiotu publicznego o udostępnienie informacji publicznej. Wynika to z przyjęcia założenia, że skoro instytucje publiczne są finansowane przez obywateli i to oni są suwerenem, na rzecz których administracja publiczna działa, to mają oni prawo wiedzieć jak i jakie procesy są realizowane w tego rodzaju instytucjach i są uprawnieni do zapoznawania się z wytwarzanymi dokumentami. Takie szerokie podejście z jeden strony zapewnia transparentność i rozliczalność działań państwa, ale z drugiej strony stanowi zagrożenie upublicznieniem danych, które z uwagi na bezpieczeństwo narodowe lub innego rodzaju bezpieczeństwo nie powinny ujrzeć światła dziennego.

Dlatego też ustawodawca wprowadził odpowiednie ograniczenia. Jeśli chodzi o cyberbezpieczeństwo, nie tylko przepisy ustawy o ochronie informacji niejawnych (OIN) mogą mieć zastosowanie (o ile na dany dokument/informacje została nałożona klauzula tajności), ale ustawa o krajowym systemie cyberbezpieczeństwa (ustawa o KSC) wprowadziła także specjalne mechanizmy bezpieczeństwa w zakresie ochrony wrażliwych danych, które niekoniecznie są klauzulowane w myśl OIN.

Warto przypomnieć o możliwości zastosowania tych przepisów, gdyż do Ministerstwa Cyfryzacji docierają informacje o masowych wnioskach do podmiotów publicznych o dostęp do informacji publicznej, które dotyczą wrażliwych i szczegółowych danych związanych z cyberbezpieczeństwem tych podmiotów oraz ochroną danych w tych podmiotach.

W takich sytuacjach wnioski te należy rozpatrywać z uwzględnieniem następujących przepisów ustawy o KSC:

- art. 37 ust. 1: *Do udostępniania informacji o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentów nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902).*

lub

- art. 38: *Nie udostępnia się informacji przetwarzanych na podstawie ustawy [o KSC], jeżeli ich ujawnienie naruszyłoby ochronę interesu publicznego w odniesieniu do bezpieczeństwa lub porządku publicznego, a także negatywnie wpłynęłoby na prowadzenie postępowań przygotowawczych w sprawie przestępstw, ich wykrywania i ścigania*.

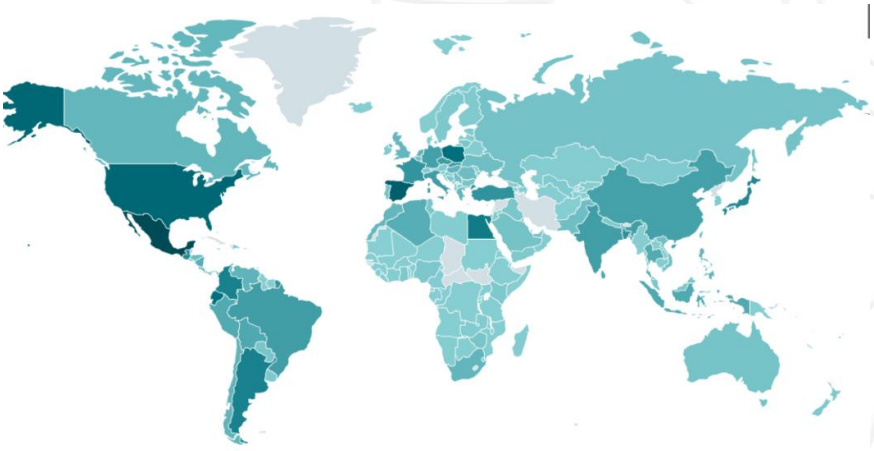
Ocena czy wyżej wymienione przepisy mają zastosowanie w danym przypadku należy do podmiotu, do którego został złożony wniosek o dostęp do informacji publicznej. Niemniej, w przypadku uwiarygodnionego przypuszczenia (np. na podstawie zakresu wnioskowanych informacji), że zdobycie tych informacji związane jest z próbą:

- identyfikacji niedostatecznie dobrze zabezpieczonych podmiotów,
- identyfikacji potencjalnych luk w konkretnych procedurach i rozwiązaniach używanych przez podmioty,
- ➢ w celu późniejszego przeprowadzenia ataku na podmiot, np. o charakterze wyłudzającym pieniądze za zaszyfrowane dane (ransomware) przez grupy przestępcze albo przez grupy o charakterze wywiadowczym, sabotażowym lub dezinformacyjnym sponsorowane przez aktorów państwowych (APT),

może dać podstawę do odpowiedniego zastosowania art. 37 ust. 1 lub art. 38 ustawy o KSC, a w efekcie ustrzec przed udostępnieniem wrażliwych danych.

Globalna operacja przeciwko Lumma Stealer

Lumma Stealer to jeden z najgroźniejszych stealerów typu Malware-as-a-Service (MaaS), który stanowi poważne zagrożenia dla użytkowników na całym świecie. Oprogramowanie to w ciągu ostatnich dwóch lat atakowało systemy użytkowników prywatnych, firm czy instytucji, wykradając wrażliwe dane takie jak hasła, pliki cookies z przeglądarek, tokeny discord czy dane z portfeli kryptowalutowych. Subskrypcja narzędzia kosztowała od 250 do 1000 dolarów, w zależności od poziomu dostępu i zaawansowania funkcji. Model subskrypcji zapewniał dostęp do najnowszych wersji malware a także do infrastruktury do wyprowadzania danych. Lumma Stealer był dystrybuowany głównie poprzez phishing, złośliwe oprogramowanie, fałszywe witryny GitHuba, często wykorzystywano również inne narzędzia jako loader. W okresie od lipca 2024 r. infostealer intensywnie targetował m.in. użytkowników z Meksyku (7,41% wszystkich ataków), Hiszpanii (5,42%), USA (4,60%) oraz Polski (3,78%). Lumma Stealer był stale rozwijany i udoskonalany. W ciągu ostatniego roku zmieniano metody szyfrowania (z prostego XOR i base64 na ChaCha20), strukturę identyfikatorów afiliacyjnych (z LID na UID), oraz dynamiczne konfiguracje złośliwego kodu. W kodzie wykorzystywano również zaawansowane techniki obfuskacji, takie jak ukrywanie ciągów znaków w stosie (stack strings) czy tzw. indirect control flow flattening – wszystko po to, by utrudnić analizę i wykrycie przez systemy bezpieczeństwa.



Źródło: welivesecurity

W odpowiedzi na eskalacje działań stealera rozpoczęto szeroko zakrojoną operację z udziałem Microsoft, Eset, Cloudflare, Europol czy japońskiego Cybercrime Control Center. Działania koordynowano w celu przejęcia infrastruktury C&C (command and control), identyfikacji serwerów używanych do wykradania danych, a także neutralizacji kanałów dystrybucji malware. Firma ESET dostarczyła analizę techniczną dziesiątek tysięcy próbek malware, co pozwoliło zidentyfikować ponad 3300 unikalnych domen C&C. W wyniku wspólnej operacji udało się unieszkodliwić znaczną część infrastruktury Lumma Stealer, co poważnie ograniczyło jego zdolność do komunikacji z zainfekowanymi urządzeniami. Działania te doprowadziły do przejęcia i dezaktywacji kluczowych elementów systemu wykorzystywanego przez cyberprzestępców. Choć nie można wykluczyć prób odbudowy infrastruktury, operacja istotnie utrudniła dalsze funkcjonowanie tego zagrożenia.
Operacja przeciwko Lumma Stealer jest ważnym sygnałem dla środowisk cyberprzestępców, że współpraca między sektorem publicznym a prywatnym może skutecznie zakłócić i ostatecznie zneutralizować nawet najbardziej zaawansowane modele czy narzędzia.

Źródła: welivesecurity.com, com, eset.com, europol.europa.eu

„Parasol Wyborczy" - podsumowanie

W czerwcu 2025 roku zakończył się trwający niemal trzy lata cykl wyborczy w Polsce, obejmujący wybory parlamentarne w 2023 roku, samorządowe oraz do Parlamentu Europejskiego w 2024 roku oraz prezydenckie w 2025 roku. Intensywność tych procesów demokratycznych w krótkim okresie stworzyła bezprecedensowe wyzwania w zakresie ochrony przed zagrożeniami w środowisku cyfrowym

Cykl ten, zbiegł się z nasilonymi napięciami geopolitycznymi, w tym rywalizacją USA–Chiny, konfliktem Rosja–Ukraina oraz eskalacją antagonizmów na Bliskim Wschodzie. Cyberprzestrzeń stała się głównym polem realizacji interesów państw i miejscem zarówno operacji wpływu (soft power) oraz ataków na infrastrukturę teleinformatyczną i komunikacyjną (ICT). Działania te są często prowadzone w sposób niejawny przez wyspecjalizowane zespoły techniczne i służby specjalne, co utrudnia a często uniemożliwia identyfikację sprawców.

Analizy minionych procesów wyborczych w krajach zachodnich i USA uwypukliły znaczenie bezpieczeństwa teleinformatycznego oraz wskazały potrzebę przeciwdziałania dezinformacji jako kluczowych elementów ochrony procesów demokratycznych. Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa wskazuje, że w Polsce w 2024 roku CSIRTy poziomu krajowego zarejestrowały 111 660 potwierdzonych incydentów teleinformatycznych, co stanowi wzrost o 23% r/r.

W odpowiedzi na rosnące zagrożenia w lutym 2025 roku uruchomiono program „Parasol Wyborczy", koordynowany przez Ministerstwo Cyfryzacji i MSWiA. Główne komponenty programu to:

- Monitoring polskiej infosfery: analiza i przeciwdziałanie dezinformacji w mediach społecznościowych, także finansowanej spoza granic Polski.
- Współpraca z platformami: koordynacja z Facebookiem, X, Instagramem, TikTokiem i innymi w celu ograniczania zasięgu szkodliwych treści.
- Monitoring przepływów finansowych: identyfikacja nielegalnych płatności i finansowania kampanii z zagranicy.
- Szkolenia i edukacja: cykl szkoleń dla komitetów wyborczych, dziennikarzy i organizatorów wyborów oraz materiały dla obywateli.
- Współpraca ze służbami specjalnymi: działania ABW obejmujące testy bezpieczeństwa systemów w KBW, szkolenia i ocenę ryzyka wywiadowczego.

Wdrożenie rozwiązań technologicznych, edukacyjnych i współpracy międzysektorowej zaowocowało zwiększeniem odporności procesów wyborczych na ataki cyfrowe i manipulacje informacyjne. Jednocześnie doświadczenia „Parasola Wyborczego" wskazują, że skuteczna ochrona demokracji wymaga stałego monitoringu, elastyczności reagowania oraz ciągłego podnoszenia świadomości społecznej.

Patrząc w przyszłość, utrzymanie i rozwój takich inicjatyw jak „Parasol Wyborczy" będą niezbędne, by sprostać ewoluującym zagrożeniom cyfrowym oraz zapewnić obywatelom transparentne i bezpieczne wybory.

S46 – centralny system wspierający cyberbezpieczeństwo podmiotów objętych KSC

System S46 został uruchomiony 1 stycznia 2021 r. na mocy art. 46 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r. Przepis ten stanowił fundament do projektowania poszczególnych funkcji Systemu, a nowelizacja ustawy rozszerza ten katalog. S46 jest platformą w portfolio Ministerstwa Cyfryzacji rozwijaną i utrzymywaną przez NASK-PIB.

Czym będzie S46?

Nowe logo Systemu S46

System S46 i jego funkcjonalności są aktualnie w procesie dynamicznych zmian – od front-endu po back-end rozwiązania. Proces ten jest odpowiedzią na nowelizację ustawy o KSC i w konsekwencji, potrzebę wprowadzenia nowych funkcjonalności oraz sprostaniu wyzwania znacznego, spodziewanego przyrostu użytkowników. Funkcje określa również sam przepis projektowanej ustawy.

Art. 46

1. Minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:

1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;

2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;

3) zgłaszanie i obsługę incydentów;

4) szacowanie ryzyka na poziomie krajowym;

5) ostrzeganie o cyberzagrożeniach;

6) czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa;

7) dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679 i art. 44 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206) przez podmioty kluczowe i podmioty ważne;

8) wymianę informacji o aktach ministra właściwego do spraw informatyzacji, Pełnomocnika, organów właściwych do spraw cyberbezpieczeństwa oraz Prezesa Rady Ministrów, o których mowa w art. 33 ust. 4, art. 42 ust. 1 pkt 5, art. 45 ust. 3, art. 67, art. 67a, art. 67b ust. 15, art. 67g ust. 1 i art. 67l ust. 1.

1a. W systemie teleinformatycznym prowadzi się wykaz podmiotów kluczowych i podmiotów ważnych.

Fragment projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa

Dodatkowo w ramach projektowanych zmian, zostanie udostępniona nowa aplikacja – **Rejestr KSC**, w której będzie prowadzony wykaz podmiotów kluczowych i ważnych.

Dla kogo?

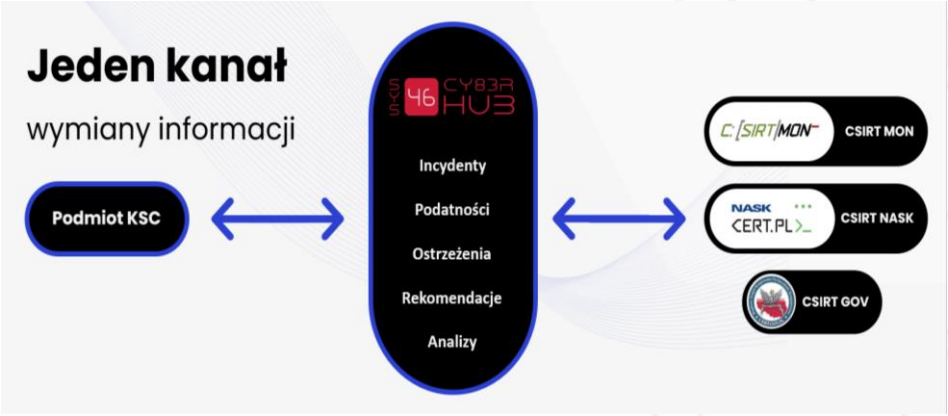
System przeznaczony jest dla podmiotów objętych ustawą o krajowym systemie cyberbezpieczeństwa, jednak w perspektywie planowane jest otwarcie dla większej liczby interesariuszy. Po nowelizacji ustawy, grono uczestników Systemu znacząco się poszerzy.

Jakie funkcjonalności?

System S46 ma za zadanie wspierać użytkowników w realizacji obowiązków określanych w ustawie o KSC, głównie z zakresie zgłaszania incydentów. S46 zapewni kanał do obsługi incydentu i proces informowania do właściwego CSIRT-u. Zapewni również dostęp do alertów, ostrzeżeń oraz różnych źródeł informacji pozwalających na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania przed tymi zagrożeniami. **W skrócie użytkownik otrzyma: wsparcie w obsłudze incydentów, informacje o podatnościach, analizy techniczne przygotowywane przez ekspertów, ostrzeżenia o zagrożeniach, feedy informacyjne, dostęp do raportów dot. cyberbezpieczeństwa.**

Podmioty i interesariusze Systemu S46 po nowelizacji ustawy o KSC

Planowane i rozwijane są również dodatkowe funkcjonalności takie jak m.in. umożliwienie śledzenia podatności (CVE) dla używanych systemów i rozwiązań przez podmioty, czy też większy dostęp do informacji o podatnościach. W perspektywie planowane jest także udostępnienie API systemu, w tym również do modułu incydentów, a dokładniej integracji z systemami ticketowymi w celu odbierania / przekazywania informacji o incydentach. Zapotrzebowanie na usługi jest analizowane w oparciu o ankiety rozsyłane cyklicznie do użytkowników, feedback zbierany podczas prezentacji oraz bezpośrednie rozmowy z użytkownikami Systemu, tak aby projektowane, kolejne funkcjonalności jak najlepiej dostosować do oczekiwań odbiorców i maksymalnie ułatwić im korzystanie z Systemu.



Wymiana informacji w S46 między podmiotami – uczestnikami Systemu, a właściwym CSIRT

Jak dołączyć?

Podmioty zainteresowane dołączeniem do S46 muszą wypełnić formularz kontaktowy dla realizacji Porozumienia oraz wypełnić oświadczenie woli. Co istotne, należy również wpisać podmiot do 'Rejestru KSC'. Po pozytywnej weryfikacji, dostęp do Systemu zostaje przyznany. **Ważnym elementem, który znacząco usprawni proces przyłączania kolejnych użytkowników jest zmiana modelu przyłączania. Uruchomiono nową metodę logowania do S46 za pośrednictwem Węzła Krajowego**, zamiast podłączania do S46 za pomocą systemu brzegowego użytkownika (SBU), gdzie konieczna była dzierżawa dwóch niezależnych łączy przez użytkownika, a urządzenie musiało być dodatkowo instalowane w jego serwerowni. Proces uzyskiwania dostępu został dzięki temu uproszczony i skrócony.

Dodatkowo NASK PIB zapewnia szkolenia: podstawowe, uzupełniające, zaawansowane, aby odpowiedzieć na potrzeby wszystkich użytkowników Systemu S46. Ponadto otrzymują oni dostęp do materiałów szkoleniowych w ramach dedykowanego portalu z bazą wiedzy o Systemie S46.

Idea utworzenia Systemu, który wspiera podmioty w realizacji wymogów związanych z ustawą o KSC jest właściwa, natomiast, aby System spełniał oczekiwania użytkowników, należy stale go rozwijać i dostosowywać do dynamicznych zmian technologicznych. Dodatkowo ważnym czynnikiem jest maksymalne skrócenie czasu uzyskiwania dostępu do Systemu przez nowych użytkowników oraz łatwe logowanie i dostępność dla obecnych.

Dostęp do narzędzi, wiedzy i zasobów cyberbezpieczeństwa dla obywateli i podmiotów powinien być prosty i zrozumiały, dlatego równolegle do procesu rozwoju i transformacji S46 prowadzony jest projekt **cyber.gov.pl** – jednej platformy skupiającej wszystkie ogólnodostępne kluczowe usługi i narzędzia z zakresu cyberbezpieczeństwa w tym zapewniającej dostęp do S46.

Logo cyber.gov.pl

17 podejrzanych za oszustwa typu Business Email Compromise (BEC) w rękach policjantów CBZC. Na rachunkach bankowych zabezpieczono ponad 21 mln zł

Obszerne, operacyjne działania policjantów Zarządu w Warszawie CBZC doprowadziły do rozbicia zorganizowanej grupy przestępczej, która podszywając się pod podmioty gospodarcze z całego świata, oszukiwała pracowników firm, bądź ich klientów i nakłaniała do wykonania określonych działań – płatności lub ujawnienia danych.

Policjanci realizowali działania na terenie województwa mazowieckiego, pomorskiego i dolnośląskiego. Dokonali 24 przeszukań, podczas których zabezpieczyli m.in. telefony, laptopy, nośniki danych, karty bankomatowe, karty SIM oraz mienie o wartości 400 tys. złotych i gotówkę w kwocie ponad 114 tys. złotych. W ramach działań operacyjnych policjanci zabezpieczyli także niezrealizowany czek bankowy na niemal milion dolarów. W ramach postępowania, na rachunkach bankowych na wniosek policjantów, prokurator zabezpieczył ponad 21 mln złotych. Ponad to policjanci ujawnili i zabezpieczyli także środki odurzające w postaci marihuany i metamfetaminy.

W sprawie zatrzymano 17 osób. Sąd zadecydował o zastosowaniu środka zapobiegawczego w postaci tymczasowego aresztu wobec 11 osób, natomiast wobec pozostałych 8 zastosowano dozór policyjny.

Zatrzymani usłyszeli odpowiednio zarzuty kierowania i udziału w zorganizowanej grupie przestępczej i prania pieniędzy, za co grozi kara do 15 lat pozbawienia wolności.

Sprawę nadzoruje Prokuratura Okręgowa Warszawa Praga w Warszawie.

Funkcjonariusze Zarządu w Warszawie CBZC działali przy wsparciu swoich komórek terenowych oraz WPS KSP i przewodnika psa z WWP KSP, Zespołu Specjalnego Zarządu we Wrocławiu CBŚP, funkcjonariuszy Wydziału IX Zarządu Operacyjno -Śledczego KG SG, CPK BOA KGP, żołnierzy Zarządu II KG ŻW, Oddziału Specjalnego ŻW w Warszawie, a także funkcjonariuszy WK i przewodnika psa z KMP w Jeleniej Górze. Łącznie w realizacji brało udział ponad 100 funkcjonariuszy.

Źródło: CBZC

Wspólne działania CBZC i KAS - rozbicie grupy przestępczej, która pod przykrywką działalności charytatywnej wyłudziła niemal 15 milionów złotych!

Funkcjonariusze Zarządu we Wrocławiu Centralnego Biura Zwalczania Cyberprzestępczości i Dolnośląskiego Urzędu Celno-Skarbowego zatrzymali właścicieli fundacji, którzy wykorzystując ludzką wrażliwość i chęć niesienia pomocy, żerowali na krzywdzie dzieci.

Wrocławski Zarząd CBZC wspólnie z Dolnośląskim Urzędem Celno-Skarbowym, rozbił zorganizowaną grupę przestępczą, która pod przykrywką działalności charytatywnej wyłudziła blisko 15 milionów złotych. Pomoc dla chorych dzieci okazała się przykrywką dla bezwzględnego biznesu. To miała być fundacja niosąca nadzieję i wsparcie. Zamiast tego była dobrze zaplanowaną machiną oszustwa.

CBZC i Służby Skarbowe rozbiły kolejną fałszywą narrację „dobroczynności".

Funkcjonariusze CBZC i Dolnośląskiego Urzędu Celno-Skarbowego w ramach pracy operacyjnej ujawnili i zatrzymali osoby stanowiące trzon zorganizowanej grupy przestępczej, który był odpowiedzialny za wieloletnie wyłudzanie pieniędzy pod pozorem pomocy chorym i niepełnosprawnym dzieciom. Od 2016 roku organizacja zebrała prawie 15 milionów złotych. Zatrzymani stosowali manipulację – wzbudzali współczucie, prowadząc działalność pod hasłami dobroczynności. Do prowadzenia fałszywych zbiórek zatrudniali osoby bezdomne, które po odbyciu „szkolenia" nauczone były, jak rozmawiać z potencjalnymi darczyńcami , jak wzbudzać litość i jak unikać odpowiedzi na niewygodne pytania.

Celem zbiórek była pomoc osobom w trudnej sytuacji rodzinnej i zebranie pieniędzy na leczenie chorych dzieci. Przeraża fakt, że przestępcy wykorzystali wizerunek dziecka, które już dawno temu przegrało z chorobą. Mimo to organizacja nadal „pomagała", pokazując w Internecie wzruszające historie dotyczące tego dziecka i opłacając rachunki na symboliczne kwoty, tylko po to, by móc wykazać aktywność na koncie. Ponadto w jednym z przeszukanych mieszkań, funkcjonariusze wykryli również znaczne ilości substancji psychotropowych, przygotowanych do dystrybucji.

Oszuści wypłacali w gotówce pieniądze z datków lub przelewali je na rachunki bankowe. Lokowali pieniądze w luksusowe nieruchomości i pojazdy.

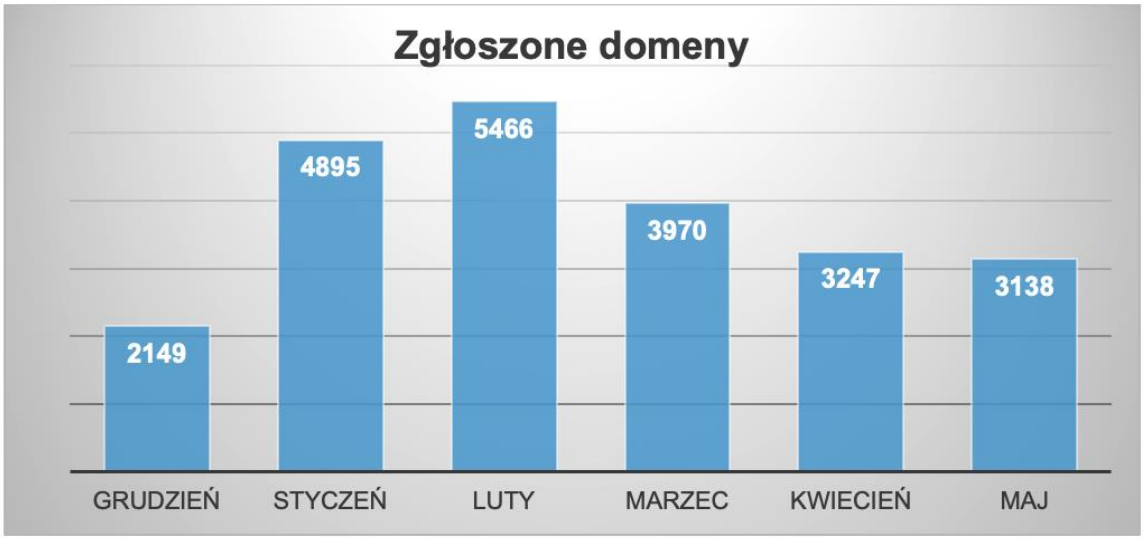
Łącznie zatrzymano 4 osoby w wieku od 34 do 74 lat – wcześniej znane organom ścigania z tytułu popełnianych przestępstw przeciwko mieniu. Przedstawiono im zarzuty udziału w zorganizowanej grupie przestępczej, prania pieniędzy, wprowadzania do obrotu środków odurzających oraz licznych oszustw podatkowych. Funkcjonariusze zabezpieczyli mienie na ponad 2 mln złotych oraz środki pieniężne na rachunkach bankowych i w gotówce. Sprawcom grozi do 12 lat pozbawienia wolności.

Wobec 3 podejrzanych Sąd Rejonowy zastosował środki zapobiegawcze w postaci tymczasowych aresztowań na okres trzech miesięcy. Sprawę nadzoruje Prokuratura Okręgowa we Wrocławiu.

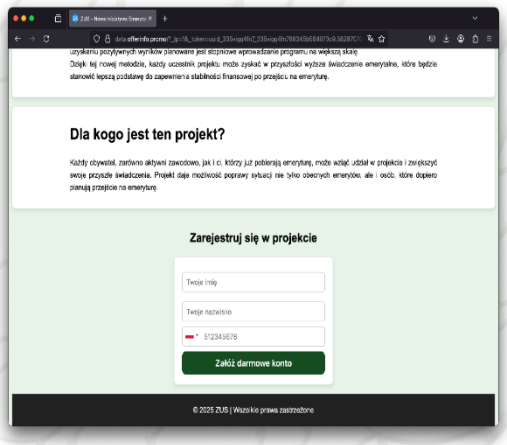
Źródło: CBZC

Podsumowanie miesiąca przez CSIRT KNF – Ochrona klienta

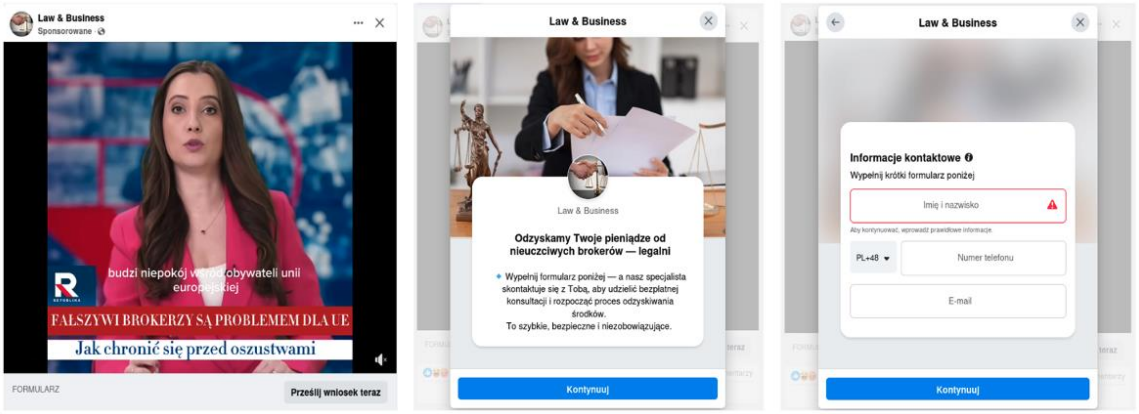
W maju 2025 roku CSIRT KNF wykrył i zgłosił do zablokowania 3 138 domen, które wcześniej zakwalifikowane zostały jako wyłudzające dane (loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe).



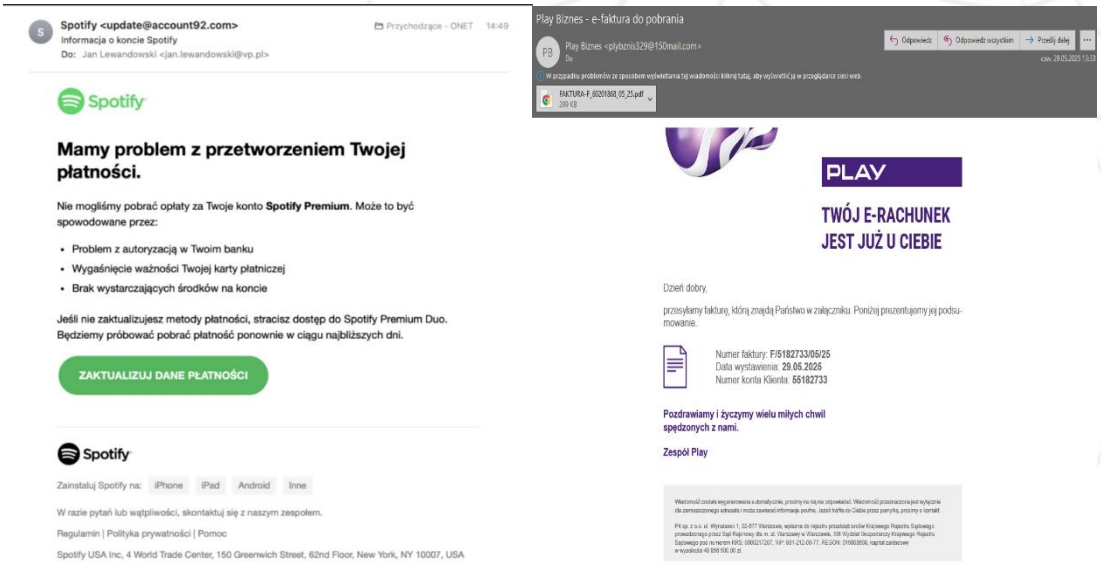
Podobnie jak w poprzednich miesiącach, również w maju 2025 kontynuowane były kampanie znane pod nazwą „fraud inwestycyjny". Przestępcy wykorzystywali wizerunek m.in. Zakładu Ubezpieczeń Społecznych, tworząc fałszywe artykuły i formularze rejestracyjne, aby nakłonić ofiary do podania danych kontaktowych, a następnie doprowadzić do strat finansowych.



W ramach drugiego etapu kampanii pojawiały się również fałszywe oferty 'odzyskiwania utraconych środków', będące de facto próbą ponownego oszustwa tych samych osób.



W analizowanym miesiącu przestępcy nadal podszywali się bezpośrednio pod banki i inne znane instytucje. W kampaniach phishingowych wykorzystywali wizerunki: Santander Bank Polska, Pocztex, home.pl, Play, Spotify, Facebook oraz DPD. Rozsyłali wiadomości SMS oraz e-mail, które prowadziły do fałszywych stron logowania lub stron wyłudzających dane kart płatniczych.



Kolejnym zagrożeniem minionego miesiąca zagrożeniem była kampania z wykorzystaniem złośliwej aplikacji mobilnej 'IKO Lokata', która podszywała się pod oficjalną aplikację bankową. Po instalacji na urządzeniach z systemem Android aplikacja wymuszała nadanie uprawnień Dostępności, co umożliwiało przejęcie kontroli nad urządzeniem i wyłudzenie danych logowania do bankowości elektronicznej.

Zachęcamy także do zapoznania się z bieżącą analizą kampanii, a także potencjalnymi konsekwencjami zainstalowania złośliwej aplikacji na urządzeniu.

Materiał dostępny jest tutaj:
https://cebrf.knf.gov.pl/images/IKO%20Lokata%20Malware%20-%20Analiza.pdf

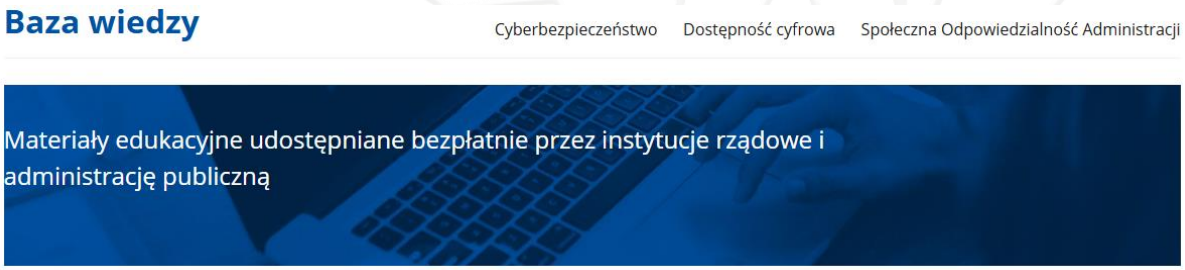
Przypominamy – jedną z najskuteczniejszych metod ochrony jest wiedza! Zachęcamy zatem do śledzenia kanałów CSIRT KNF w mediach społecznościowych (X, LinkedIn, Facebook) oraz do zapoznania się z pełnym raportem miesięcznym na stronie: https://cebrf.knf.gov.pl/

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

Źródło: *nask.pl*

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.