Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

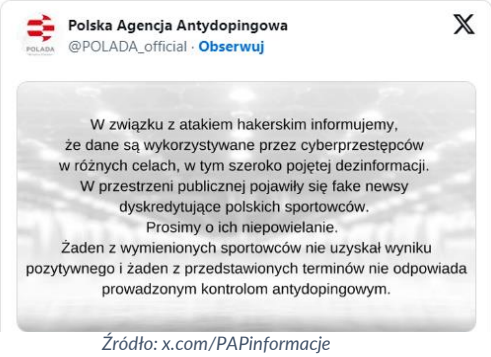
ZAGROŻENIA W CYBERPRZESTRZENI

08/2024

SPIS TREŚCI

Atak hackerski na Polską Agencję Antydopingową

W dniu 06 sierpnia br. w czasie trwania odwiecznego święta sportu - igrzysk olimpijskich w Paryżu, oczy widzów z całego świata skierowane były na rywalizację sportową przedstawicieli wszystkich nacji... tzn. prawie wszystkich. W tegorocznych igrzyskach w związku z agresją na Ukrainę zabrakło wykluczonych przez MKOL reprezentantów Białorusi oraz Rosji. MKOL nałożył na Rosję sankcje, nazywając ten akt „rażącym naruszeniem" trwającego od wieków rozejmu olimpijskiego, który przewiduje okres pokoju rozpoczynający się siedem dni przed igrzyskami olimpijskimi i kończący się siedem dni po igrzyskach paraolimpijskich. Ponadto, we wspominanym dniu grupy cyberprzestępcze powiązane z Rosją ujawniły udany atak hackerski na *Polską Agencję Antydopingową* (POLADA). Zgodnie z przedstawionymi informacjami na kanale *Telegram* dwóch rosyjskich grup haktywistycznych (celowo nie podajemy nazw) upubliczniono niespełna 243 GB wrażliwych danych (m.in. osobowe, medyczne, wyniki badań antydopingowych) polskich sportowców. Mowa o blisko 50 tys. plikach pochodzących z komputerów POLADA oraz z serwera wirtualnego organizacji. Ponadto hakerzy obrali na cel stronę internetową *antydoping.pl* (strona POLADA), czasowo wyłączając ją z użytkowania. Analizując metadane plików udostępnionych przez włamywaczy, należy zakładać, że dane zostały wykradzione w ostatnich dniach kwietnia br. Na podstawie informacji zawartych w materiale wideo w przekazanym przez atakujących widać, że hasło do zarządzania serwisem było przechowywane na zainfekowanym komputerze jednego z pracowników POLADA'y w niezaszyfrowanym dokumencie MS Word.



Źródło: x.com/PAPinformacje

POLADA w oficjalnym komunikacie stwierdza *„ustalenia wskazują, że atak jest działaniem grupy wspieranej przez służby wrogiego państwa"*. Skala incydentu wydaje się zatrważająca, nie tylko ze względu na swoją wielkość, ale również charakter i czas publikacji materiałów. Sprawę badają *CERT Polska* oraz CBZC. Jednakże analiza techniczna ww. incydentu ze względu na zaawanasowane techniki anonimizacji i tzw. OPSEC stosowany przez grupy hackerskie wspierane przez państwo (typu *state sponsored* - do takich zalicza się grupa odpowiedzialna za ww. kanał na *Telegramie*) może uniemożliwić skuteczną atrybucję ataku. Stąd też, w takich przypadkach następuję analiza kontekstowa zdarzenia celem przypisania podmiotów odpowiedzialnych za incydent. W tym przypadku jednoznacznie zbieżny z polityką aktywności hybrydowej w przestrzeni cyfrowej rosyjskich służ specjalnych. Atak miał na celu dyskredytacje polskich sportowców na arenie międzynarodowej, co miało bezpośrednio rzutować na ocenę Polski jako kraju. Atak przeprowadzony był z zamiarem sztucznego wykreowania szumu medialnego i wykorzystania „głośności" zdarzenia, w związku z trwającymi igrzyskami. Powyższe potwierdza nie tylko czas i charakter publikacji, ale również spreparowane w sposób niedbały materiały (o negatywnym nacechowaniu) dot. danych polskich sportowców stanowiących światową czołówkę w swoich dyscyplinach, co jednoznacznie wskazuje na dezinformacyjny/hybrydowy cel przeprowadzanego ataku.

Źródła: rp.pl, zaufanatrzeciastrona.pl, pap.pl

Standardy NIST dla szyfrowania postkwantowego

NIST (*Narodowy Instytut Norm i Technologii, USA*) opublikował finalny zestaw narzędzi szyfrujących, które mają zabezpieczać informacje przed atakami komputerów kwantowych. Nowe standardy opracowane w ramach projektu kryptografii postkwantowej (PQC), mają na celu ochronę szerokiego zakresu informacji elektronicznych, od poufnych wiadomości e-mail po transakcje *e-commerce*. Administratorom systemów komputerowych zaleca się, jak najszybsze wdrażanie tych standardów. Nowe standardy są stworzone z myślą o przyszłości. Technologia komputerów kwantowych rozwija się szybko, a niektórzy eksperci przewidują, że urządzenie zdolne do złamania obecnych metod szyfrowania może pojawić się w ciągu dekady, zagrażając bezpieczeństwu i prywatności osób, organizacji oraz całych państw.

Finalne standardy obejmują:

- *FIPS 203* - Standard szyfrowania ogólnego oparty na algorytmie *CRYSTALS-Kyber*, charakteryzuje się szybkością i małymi kluczami szyfrowania.
- *FIPS 204* - Standard ochrony podpisów cyfrowych oparty na algorytmie *CRYSTALS-Dilithium*,
- *FIPS 205* - alternatywny standard podpisów cyfrowych oparty na algorytmie *Sphincs+*, przeznaczony jako zapasowa metoda szyfrowania.

W przyszłości planowany jest także ***FIPS 206***, oparty na algorytmie *FALCON*.

Nowe standardy mają kluczowe znaczenie dla ochrony prywatności i bezpieczeństwa w obliczu rosnącego zagrożenia ze strony komputerów kwantowych. NIST kontynuuje pracę nad dodatkowymi zestawami algorytmów, które mogą stać się alternatywnymi standardami w przyszłości, aby zapewnić bezpieczeństwo w przypadku złamania aktualnych metod.

Unia Europejska wydała 11 kwietnia 2024 r. Zalecenia Komisji 2024/1101 dot. wspierania przejścia na kryptografię postkwantową, aby chronić infrastrukturę cyfrową i usługi publiczne w UE przed zagrożeniami ze strony komputerów kwantowych. Komisja zachęca państwa członkowskie do stworzenia skoordynowanego planu wdrożenia, który będzie obejmował wybór odpowiednich algorytmów kryptografii postkwantowej oraz ich wprowadzenie w systemach administracji publicznej i infrastrukturach krytycznych. Zalecenie promuje współpracę na poziomie unijnym i międzynarodowym w celu harmonizacji standardów, interoperacyjności oraz monitorowania postępów, co ma zabezpieczyć kluczowe systemy przed przyszłymi zagrożeniami kwantowymi.

Warto również wspomnieć o polskim wkładzie w kryptografię post kwantową i generatorze kluczy opracowanym przez *Politechnikę Warszawską*. Generowane klucze są głęboko ukryte w elektronice i przywoływane jedynie na moment ich użycia, by następnie zniknąć z systemu. Generator wykorzystuje tzw. efekt motyla, a więc sytuacje gdy zachodzące zmiany są zbyt złożone by można je było przewidzieć. Wynalazek uzyskał pierwszy na uczelni europejski patent o jednolitym skutku prawnym, chroniący go automatycznie w 17 krajach UE. Technologia jest przeznaczona zarówno do profesjonalnych systemów kryptograficznych, jak i popularnych urządzeń, takich jak Internet Rzeczy (IoT).

Źródła: nist.gov, european-union.europa.eu, pw.edu.pl

Strategicznie o cyberbezpieczeństwie w NATO i UE –

W poprzednim Biuletynie pisaliśmy o rekomendacjach prezydenckich do nowej Strategii Bezpieczeństwa Narodowego RP. W tym miesiącu pochylimy się nad strategicznymi kierunkami w zakresie cyber wyznaczanymi w NATO i UE.

Na szczycie Sojuszu Północnoatlantyckiego w Waszyngtonie w lipcu br. przyjęto Deklarację, która w 38 punktach określa najważniejsze zamierzenia. Wśród nich znalazł się szereg kwestii dotyczących cyberbezpieczeństwa. W dokumencie podkreślono rosnące zagrożenia, w tym pogłębiające się strategiczne partnerstwo między Rosją a Chinami, w związku z czym NATO staje w obliczu zagrożeń hybrydowych, cyber, kosmicznych i innych.

Podkreślono znaczenie działań w zakresie odstraszania i obrony, w tym dokonywanej sojuszniczej transformacji cyfrowej oraz integracji nowych technologii i innowacji. NATO tworzy Zintegrowane Centrum Cyberobrony, aby zwiększyć ochronę sieci, świadomość sytuacyjną oraz wdrażanie cyberprzestrzeni jako domeny operacyjnej w czasie pokoju, kryzysu i konfliktu, jak również opracowuje politykę zwiększającą bezpieczeństwo sieci NATO. Podkreślono, że operacje hybrydowe mogą osiągnąć poziom ataku zbrojnego i uruchomić artykułu 5 Traktatu Waszyngtońskiego. Wdrożone zostaną m.in. zrewidowana Strategia AI i Strategia Kwantowa oraz rozwijane będą Sojuszniczy Akcelerator Innowacji Obronnych DIANA i Fundusz Innowacji NATO (NIF). Kolejnym ważnym elementem jest zapowiedź dalszego rozwoju indywidualnych i zbiorowych zdolności do analizy i przeciwdziałania wrogim operacjom dezinformacyjnym, dzielenia się informacjami oraz współpracy w zakresie komunikacji strategicznej.

Tzw. "Family photo" przywódców państw na szczycie NATO w Waszyngtonie w lipcu 2024. Źródło: NATO

Z kolei przewodnicząca Komisji Europejskiej, która w nowej kadencji kontynuuje swą misję, przedstawiła orędzie o stanie Unii, w którym wskazane zostały priorytety nowej KE na lata 2024-2029, w śród nich podniesiono także szereg spraw z zakresu cyberbezpieczeństwa.

Komisja Europejska skupi się na dalszym wzmacnianiu zdolności do cyberobrony, koordynacji krajowych działań w cyberprzestrzeni i zabezpieczaniu infrastruktury krytycznej. Komisja przedstawi Białą Księgę w sprawie przyszłości europejskiej obronności, gdzie domena cyber będzie jednym z istotnych obszarów. Między innymi w ramach Europejskiego Funduszu Obronnego (EDF), rozwijany będzie potencjał przemysłowy we wszystkich kluczowych

obszarach zdolnościowych, w tym na polu cyber. Zaproponowanych zostanie szereg projektów obronnych stanowiących przedmiot wspólnego europejskiego zainteresowania, zaczynając od cyberobrony. Wzmocnione zostaną mechanizmy sankcyjne, w tym w zakresie sankcji przeciwko cyberatakom.

Podkreślono, iż należy zrobić więcej, aby chronić bezpieczeństwo systemów opieki zdrowotnej, które coraz częściej stają się celem cyberataków, w tym ransomware. KE zaproponuje europejski plan działania w zakresie cyberbezpieczeństwa szpitali i dostawców opieki zdrowotnej.

Powstać ma nowy Europejski System Komunikacji Krytycznej, który będzie wykorzystywany przez organy publiczne odpowiedzialne za bezpieczeństwo.

Podejmowane będą działania, aby zapewnić organom ścigania odpowiednie i aktualne narzędzia do zgodnego z prawem dostępu do informacji cyfrowych, jednocześnie chroniąc prawa podstawowe.

Grafika z dokumentu zawierającego polityczny wytyczne dla nowej Komisji Europejskiej na lata 2024-2029

Obserwowany jest wzrost liczby zagrożeń ze strony podmiotów wewnętrznych i zagranicznych – czy to wrogich rządów, czy podmiotów niepaństwowych. Zauważa się, że używane metody są teraz trudniejsze do śledzenia, bardziej szkodliwe i łatwiejsze do wdrożenia za pomocą narzędzi cyfrowych i mediów społecznościowych. Odzwierciedla to głęboką zmianę w przestrzeni informacyjnej, przejście od mediów redakcyjnych do treści generowanych przez użytkowników, przekazywanych przez platformy i promowanych przez algorytmy. Umożliwia to nowe swobody, ale także obniża koszty manipulowania informacjami i ułatwia Rosji i innym aktorom zintensyfikowanie wojny informacyjnej.

W związku z KE zaproponuje nową Europejską Tarczę Demokracji. W ramach tej inicjatywy toczyć się będą prace nad przeciwdziałaniem zagranicznej manipulacji informacjami i ingerencji w Internecie, opierając się na przykładach *Viginum* we Francji i Szwedzkiej Agencji Obrony Psychologicznej. Celem jest zwiększenie świadomości sytuacyjnej poprzez wykrywanie, analizowanie i proaktywne przeciwdziałanie dezinformacji i manipulacji informacjami. Komisja chce też się skupić na odporności i przygotowaniu społecznym poprzez zwiększenie kompetencji cyfrowych i medialnych oraz wzmocnienie zapobiegania poprzez *pre-bunking*. Stworzona zostanie europejska sieć *fact-checkerów* działająca we wszystkich językach urzędowych UE. Unia będzie również nadal zwiększać egzekwowanie prawa cyfrowego, aby zapewnić wykrywanie, oznaczanie i, w stosownych przypadkach, usuwanie zmanipulowanych lub wprowadzających w błąd informacji zgodnie z ustawą o usługach cyfrowych. KE zajmie się też coraz bardziej realistycznymi deepfake'ami, które wpłynęły na wybory w całej Europie. Zapewni też wdrożenie wymogów przejrzystości zawartych w akcie o sztucznej inteligencji i wzmocnienie naszego podejścia do treści tworzonych przez AI.

Źródło: NATO, Komisja Europejska.

Open source a cyberbezpieczeństwo

Oprogramowanie otwartoźródłowe (*open source*) posiada wiele zalet z punktu widzenia użytkownika i administratorów, jest też kluczowe dla rozwoju otwartego internetu oraz powszechnego dostępu do korzyści, jakie przynosi komputeryzacja. Jest to też ważne zagadnienie z punktu widzenia suwerenności cyfrowej państwa i możliwości jego rozwoju.

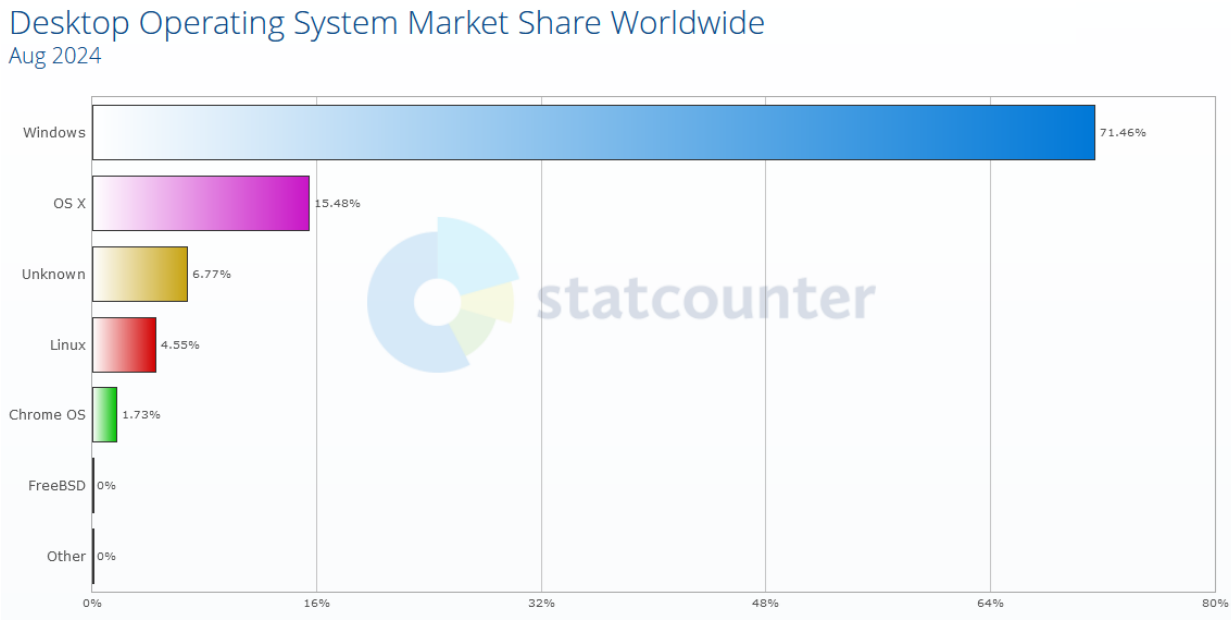
Wysoki poziom cyberbezpieczeństwa w oprogramowaniu *open source* jest możliwy dzięki otwartości kodu, co oznacz możliwość jego badania, wykrywania luk i ich szybkiego łatania, szczególnie, gdy wokół danego oprogramowania skupiona jest aktywna społeczność. Wówczas bardzo trudne byłoby utrzymywanie *backdoor*-ów, które mogą istnieć w przypadku zamkniętego oprogramowania, np. aby umożliwić dostęp służbom wywiadowczym. Bazowanie na *open source* pozwala też unikać zależności od jednego dostawcy, co zwiększa elastyczność i możliwość szybkiej reakcji na zagrożenia. Należy jednocześnie przyznać, że oprogramowanie otwartoźródłowe wiąże się też z ryzykami, takimi jak zależność od małych zespołów i pojedynczych deweloperów; ograniczone zasoby formalnego wsparcia i audytów, zależność od innych bibliotek; tworzenie różnych wersji (tzw. *forków*), które mogą być mniej stabilne; wprowadzanie fałszywych wersji do publicznych repozytoriów.

W przypadku systemów operacyjnych dostępnych jest wiele darmowych, otwartoźródłowych wersji systemu *Linux*. Jego dystrybucje często mają niższe wymagania sprzętowe, ich zaletą jest także wysoka odporność na złośliwe oprogramowanie. Poza tym dostępne jest dla nich bogate darmowe oprogramowanie również na licencji *open source*, stanowiące zamienniki dla odpłatnych rozwiązań. Również szerokie możliwości konfiguracji oraz wykorzystanie rozwiązań chmurowych należy zaliczyć do zalet takiego rozwiązania pod względem bezpieczeństwa i funkcjonalności. Na poziomie organizacji migracja do otwartoźródłowych systemów może wiązać się z pewnymi początkowymi kosztami (takimi jak koszty osobowe reinstalacji) oraz początkowymi trudnościami dla administratorów i użytkowników (z uwagi na ich przyzwyczajenia), lecz ostatecznie rozwiązania *open source* są znacznie tańsze w utrzymaniu.

Memy z grup na Facebooku poświęconych Linuxowi. Nazwy innych systemów operacyjnych zanonimizowano.

Warto podkreślić, że systemy *Linux* są relatywnie bezpieczne, gdyż większość złośliwego oprogramowania jest projektowana pod popularny komercyjny system operacyjny, więc w przypadku systemu *Linux* często po prostu ono nie zadziała. Poza tym OS z pingwinkiem uważany jest za bardziej odporny na *malware* m.in. z uwagi jego architekturę, sposób zarządzania uprawnieniami i modelu rozwoju. Szczególne znaczenie ma wspomniana kwestia otwartości kodu. Oznacza to, że każdy może go przeglądać i weryfikować pod kątem bezpieczeństwa. W rezultacie problemy i podatności mogą być szybciej wykryte i załatane, w czym pomaga szeroka społeczność tym się zajmująca.

Jeśli chodzi o indywidualnych użytkowników, systemy *Linux*, choć pozostają niszowe, to jednak w ostatnim czasie zyskują coraz większą popularność. Według badania firmy *StatCounter*, obecnie *Linux* jest postawiony na 4,45% komputerów, choć rok wcześniej było to tylko 3,18%, a dwa lata temu 2,8%. Jednym z czynników, który powodował, że pewna grupa użytkowników nie decydowała się na *Linuxa*, były ograniczone możliwości uruchamiania gier komputerowych. Jednak i tu w ostatnich latach wiele się zmieniło głównie za sprawą platformy *Steam*, która oferuje możliwość uruchamiania co raz większej liczby gier na *Linuxie* (dzięki funkcji *Proton*), jak i innych narzędzi do tego przeznaczonych, jak *Lutris*, *Wine*, czy *Heroic* oraz możliwością rozgrywki w chmurze.



Wykres pokazujący popularność systemów operacyjnych na "desktopach" w sierpniu 2024 r. Źródło: Statcounter.com

Nie są znane przypadki, że administracja całego państwa dokonała migracji do oprogramowania *open source*, niemniej pewne próby „przesiadki" na *Linuxy* odbywały się na poziomie administracji regionalnej (np. niemieckich landów) czy poszczególnych instytucji (np. francuskiej żandarmerii wojskowej). Do korzystania z oprogramowania otwartoźródłowego zachęca też Komisja Europejska.

Źródła: statcounter.com, ZDNet, WIRED, The Register.

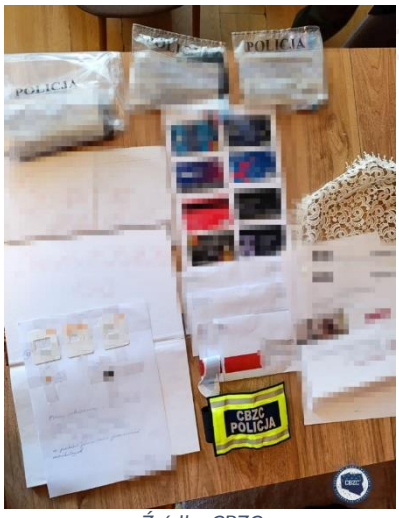
Zatrzymania w sprawie wyłudzeń pieniędzy w zamian za usuwanie negatywnych komentarzy w sieci

Policjanci Wydziału w Kielcach przy wsparciu funkcjonariuszy z Olsztyna *Centralnego Biura Zwalczania Cyberprzestępczości*, zatrzymali na terenie Elbląga cztery osoby zamieszane w proceder wyłudzania pieniędzy w zamian za usuwanie negatywnych komentarzy w sieci, dotyczących trzech kancelarii adwokackich. *Sąd Rejonowy* przychylił się do wniosku prokuratury i zastosował wobec głównego podejrzanego środek zapobiegawczy w postaci tymczasowego aresztowania na okres 3 miesięcy.

Źródło: CBZC

Wydział w Kielcach Centralnego Biura Zwalczania Cyberprzestępczości prowadzi pod nadzorem *Prokuratury Okręgowej w Kielcach*, śledztwo dotyczące zamieszczania w Internecie negatywnych komentarzy dotyczących działalności trzech kancelarii adwokackich, a następnie wyłudzaniu środków finansowych w zamian za ich usuwanie.

Śledczy z kieleckiego cyberbiura ustalili, że pokrzywdzeni adwokaci zostali doprowadzeni do niekorzystnego rozporządzenia własnym mieniem w łącznej kwocie ponad 41 tys. złotych.



Źródło: CBZC

Policjanci dotarli do mężczyzny, który kontaktował się z adwokatami, i który w rozmowie z nimi oświadczał, że otrzymywał zlecenia zamieszczenia pozytywnych i negatywnych opinii na profilach pokrzywdzonych w sieci.

Z analizy tej sprawy może wynikać, że informacja o zleceniu zamieszczenia pozytywnych jak i negatywnych komentarzy może być spreparowana przez podejrzanego w celu późniejszego wymuszania pieniędzy od pokrzywdzonych za usunięcie tych niewygodnych.

W wyniku przeprowadzonych czynności służbowych oraz realizacji postanowień prokuratora, funkcjonariusze *Wydziału w Kielcach Centralnego Biura Zwalczania Cyberprzestępczości* oraz *Zarządu w Olsztynie CBZC*, zatrzymali w sierpniu 4 osoby zamieszane w ten proceder. Policjanci przeprowadzili na terenie Elbląga liczne przeszukania pomieszczeń zajmowanych przez podejrzanych, w wyniku czego zabezpieczono nośniki danych informatycznych w postaci telefonów komórkowych, kart bankomatowych oraz umów bankowych.

Śledczy zarzucają zatrzymanym osobom przestępstwa prania pieniędzy, oszustwa oraz usiłowania wymuszenia rozbójniczego.

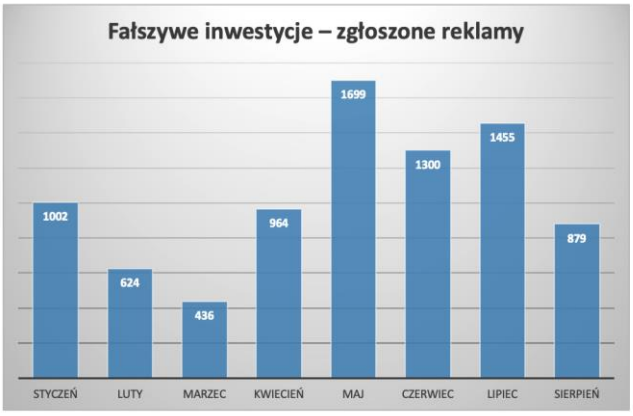
Z uwagi na grożące podejrzanym surowe kary, a także w celu zabezpieczenia prawidłowego toku prowadzonego śledztwa, *Prokuratura Okręgowa w Kielcach* zastosowała wobec trzech osób poręczenie majątkowe oraz dozór policji. Z kolei *Sąd Rejonowy w Kielcach* przychylił się do wniosku prokuratury wobec głównego podejrzanego i zastosował wobec 28-latka środek zapobiegawczy w postaci tymczasowego aresztowania na okres 3 miesięcy.

Więcej informacji pod adresem:
https://cbzc.policja.gov.pl/bzc/aktualnosci/384,Zatrzymania-w-sprawie-wyludzen-pieniedzy-w-zamian-za-usuwanie-negatywnych-koment.html

Podsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta

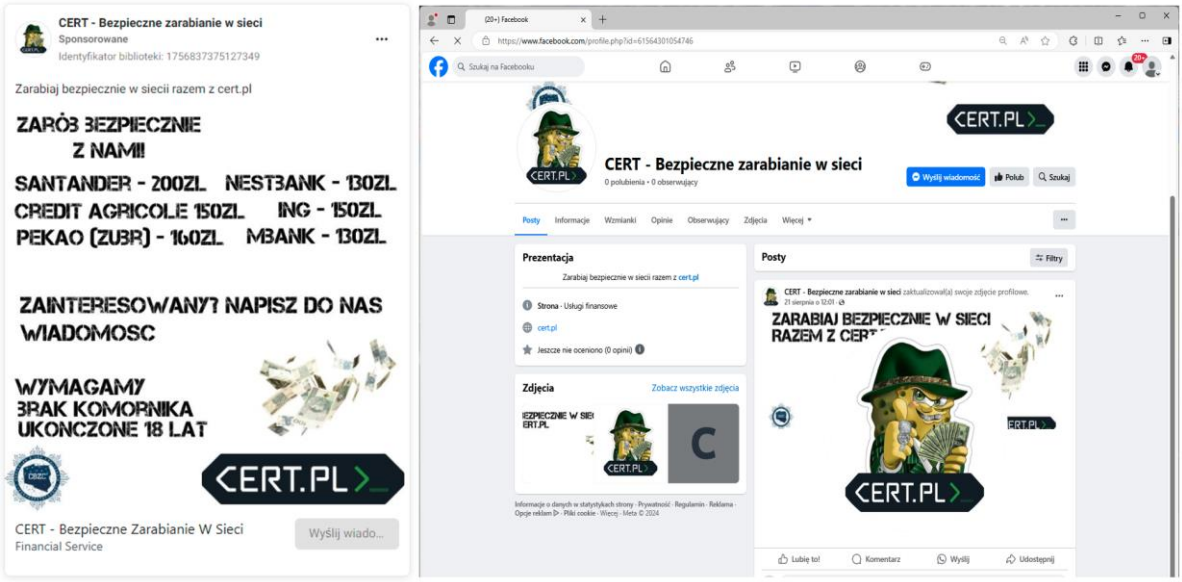
W sierpniu 2024 roku *CSIRT KNF* wykrył i zgłosił do zablokowania 3 215 domeny, które wcześniej zakwalifikowane zostały jako wyłudzające dane (m.in. loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe), dla porównania *CERT Polska* dodał na listę ostrzeżeń 6 966 domen. A na koniec omawianego miesiąca, na liście hole znajdowało się 232 146 domen.

Niezmiennie wiele osób daje się nabrać na znanych pod nazwą „fałszywe inwestycje" schemat działania przestępców. Do oszukiwania ludzi atakujący wykorzystują głównie reklamy w mediach społecznościowych. Informują one o rzekomej możliwości inwestowania, a w rzeczywistości powodujące wysokie straty finansowe u klientów banków. Jednocześnie atakujący podejmują szereg działań mających na celu utrudnienie wykrycia publikowanych przez nich materiałów. *CSIRT KNF* w trybie ciągłym pracuję nad mechanizmami wykrywającymi tego typu materiały oszukańcze. Następnie pozyskane informacje przekazywane są do odpowiednich podmiotów, celem dokonania blokady. Poniższy wykres przedstawia wykryte i zgłoszone do blokady reklamy fałszywych inwestycji na portalu Facebook, w podziale na kategorie wykorzystywanego wizerunku.



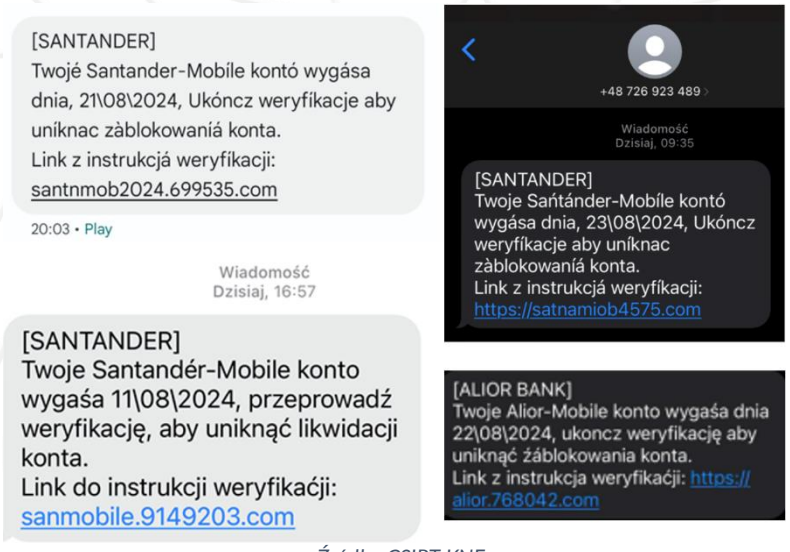
Źródło: CSIRT KNF

Dodatkowo, w sierpniu'24 roku analitycy *CSIRT KNF* wykryli i zgłosili do blokady 316 fałszywe profile (427 w lipcu'24), które publikowały fałszywe reklamy inwestycyjne. Zdarza się również, że innym sposobem na wzmocnienie prowadzanej gry psychologicznej, jest wykorzystanie wizerunku znanych instytucji, w omawianym przypadku *CERT POLSKA* oraz *CBZC*. W sierpniu 2024 przestępcy przygotowali strony podszywające się pod wspomniane organizacje. Ofiary informowali o rzekomej możliwości „bezpiecznego zarobku".



Źródło: CSIRT KNF

Podobnie jak w minionych miesiącach, atakujący przygotowali również aplikacje, mające na celu zachęcenie do rzekomego inwestowania. Aplikacje te nie infekują urządzeń. Mają na celu uwiarygodnianie scenariusza *phishingowego*. Również powtarzającym się schematem, ale niestety nadal nadbierającym wiele osób, jest drugi etap omawianego oszustwa. W nim, przestępcy publikują informację o rzekomej możliwości odzyskania utraconych wcześniej pieniędzy. W rzeczywistości, jest to ponowna próba oszukania osób, które już wcześniej dały się nabrać na ten scenariusz.



Źródło: CSIRT KNF

W sierpniu 2024 analizowaliśmy również kampanie *phishingowe* wykorzystujące wizerunek polskich banków. Strony *phishingowe* dystrybuowane były głownie poprzez wiadomości SMS.

Po kliknięciu w link ofiara trafiała na stronę *phishingową*. W ten sposób atakujący chcieli wyłudzić dane logowania do bankowości elektronicznej. Warto zwrócić również uwagę na sposób zapisów niektórych wyrazów w fałszywej wiadomości, przestępcy starają się tak unikać wykrycia dystrybucji kampanii phishingowej i niezablokowania jej przed dostarczeniem do potencjalnych ofiar.

Kolejnym schematem analizowanym w sierpniu'24 były kampanie *phishingowe* wyłudzające dane kart płatniczych. Dla przykładu, przestępcy podszywali się pod *MPK Białystok*. Pod

pretekstem rzekomej możliwości nabycia karty miejskiej, uprawniającej do nielimitowanych przejazdów, za jedyne 10zł zachęcali do kliknięcia w reklamę.

Jeżeli ktoś dał skusić się ofertą i kliknął w link, trafiła na stronę, na której proszony był o odpowiedź na kilka pytań. Następnie wyświetlał się formularz do wpisania danych osobowych oraz informacji o karcie płatniczej: numer karty, *kod CVV*, data ważności, kody *3DSecure*.

Źródło: CSIRT KNF

Jak co miesiąc mierzyliśmy się również ze znanymi od dawna schematami, takimi jak *„scam na kupującego”*, podszycia pod platformy *streamingowe*, wykorzystywanie wizerunku firm kurierskich, *Poczty Polskiej* i inne, o których poczytać można na stronie internetowej *UKNF* oraz na profilach *CSIRT KNF* w mediach społecznościowych: *X* (*Twitter*), *LinkedIn* oraz *Facebook*.

Jednocześnie zachęcamy również do zapoznania się z opublikowany raportem, który pokazuje metody i narzędzia cyberprzestępców, którzy wyłudzają pieniądze poprzez fałszywe serwisy internetowe, aplikacje mobilne, reklamy w mediach społecznościowych i *Google Ads*.

Raport dostępny pod adresem:
https://cebrf.knf.gov.pl/images/Schematy_i_metody_oszustw_inwestycyjnych.pdf

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

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.