Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

09/2024

SPIS TREŚCI

Yubikey - podatności wyłącznie dla VIPów

W minimom miesiącu pojawiło się medialne poruszenie związanie z wykryciem luki bezpieczeństwa w produktach *YubiKey* firmy *Yubico*. Rozwiązania *2FA* oparte o fizyczne klucze bezpieczeństwa, dotychczas cieszyły się mianem najwyższego poziomu ochrony dostępu do danych. Czy wykryta podatność to zmieniła?

Z upublicznionych przez producenta informacji dot. odkrycia luk bezpieczeństwa w swoich produktach wynika, iż wykryte podatności znajdują się w bibliotece kryptograficznej obsługującej klucze ECDSA (*Elliptic Curve Digital Signature Algorithm*) w mikrokontrolerze *Infineon* (podatność dotyczy następujących produktów firmy *Yubico* oraz wersji firmware *YubiKey* serii: *YubiKey serii 5 wersje przed 5.7.0*, *YubiKey 5 serii FIPS wersje przed 5.7.0*, *YubiKey 5 serii CSPN wersje przed 5.7.0*, *YubiKey serii Bio wersje przed 5.7.0*, *Security Key wersje przed 5.7.0*, *YubiHSM 2 wersje przed 2.4.0*, *YubiHSM 2 FIPS wersje przed 2.4.0).*

Klucze fizyczne. Źródło: dooball24hd.com

Na podstawie dostępnych analiz technicznych omawianej podatności, można określić potencjalną metodologię przeprowadzenia ataku wykorzystującego wykrytą lukę. Atakujący uzyskali teoretyczną możliwość tzw. sklonowania klucza fizycznego, tj. utworzenia kopii właściwości kryptograficznych urządzenia. Jednakże zgodnie z międzynarodowym standardem oceny podatności CVE - CVSS SIG (*Common Vulnerability Scoring System SIG fundacji FIRST)* wynik wynosi „4.9”, co można określić, jako o nieznacznym ryzku użycia.

Potencjalny, efektywnie przeprowadzony atak na urządzenie wymaga zaangażowania przez atakującego bardzo dużych zasobów organizacyjno-technologicznych, w tym zaawansowanych technik, narzędzi oraz posiadania wysokiego poziomu wiedzy z zakresu kryptografii i elektroniki. Wykorzystanie podatności wiąże się z koniecznością utraty przez właściciela fizycznej kontroli nad kluczem na dłuższy czas oraz znajomości przez adwersarza docelowego konta wskazanego do przejęcia, jego loginu, hasła/kodu PIN/dostępu do danych biometrycznych (w zależności od sposobu zabezpieczenia), jak i potrzebą fizycznego zniszczenia oryginalnego egzemplarza klucza. Tak opisane wymagania, których spełnienie jest niezbędne do przeprowadzenia efektywnego ataku przez adwersarza sprawia, że jest to atak możliwy do przeprowadzenia wyłącznie przez służby specjalne wrogich państwa, lub najbardziej wyrafinowane grupy przestępcze. Nie licząc zasobów wymaganej wiedzy. Sama logistyka, narzędzia i infrastruktura ataku wyceniana jest na kilkadziesiąt tysięcy złotych od klucza, co jest kwotą na tyle znaczącą, że w przypadku zwykłego obywatela prawdopodobieństwo ataku jest znikome.

W związku z powyższym, należy zaznaczyć, że fizyczne klucze bezpieczeństwa wciąż pozostają jedną z najlepszych metod ochrony naszych danych i niwelują zagrożenie przed dużą liczbą ataków (w tym m.in. *phishingiem*). Rekomendujemy stosowanie tego typu rozwiązania we wszelkich możliwych miejscach logowania. W przypadku wykorzystywania przez Państwa kluczy *YubiKey* w wersjach podatnych, zaleca się wykorzystanie dodatkowego zabezpieczenia w postaci kodu PIN/hasła/biometrii, a w dalszej kolejności ewentualną wymianę egzemplarza na rozwiązania, które nie są podatne. Takie działania zapewnią całkowite poczucie bezpieczeństwa.

Telegram – na pewno bezpieczny komunikator?

Paweł Durov, tak nazywa się twórca znanych za wschodnią granicą - portalu *VKontakcie* i wymienionego w tytule - komunikatora *Telgram*. Do niedawna, Durov posiadał status lokalnego, niedającego się złamać putinowskiemu reżimowi anarcho-liberała. Czasem nazywany był również złotym dzieckiem rosyjskiego IT lub rosyjskim Zuckerbergiem. Z tym ostatnim ma wiele wspólnego. Podobnie jak Amerykanin, który na wiele lat praktycznie zmonopolizował światowy rynek mediów społecznościowych, tak ten zawłaszczył całą rosyjskojęzyczną przestrzeń socialmediów. *VKontakcie*, jak i *Telgram* wciąż stanowią podstawowe płaszczyzny cyfrowego życia na wschód od Bugu, aż po Władywostok. Tylko czy na Wschodzie jest miejsce na cyfrową wolność? Koncepcja *Runetu*, czy polityka informacyjna Kremla, sprawia że rosyjskiemu internetowi jest bliżej do Wielkiego Brata, niż do Mateczki Rosji, choć dalej wszystko zostaje w rodzinie… dosłownie wszystko, no przynajmniej to co wrzucimy do sieci.

Logo telegram. Źródło: telegram.org

Wracając do P. Durova. PR jego „niezależnej" osoby został zbudowany na wsparciu protestów w trakcie rosyjskich wyborów prezydenckich w 2011 r., oraz odmowy kolejnych prób odsprzedaży Kremlowi swoich produktów. Działania Durova, sprawiły wrażenie, że w Rosji (FR) może funkcjonować niezależny Internet, a asertywna wobec władz postawa właściciela największych rosyjskich socialmediów dawała w świecie Zachodnim poczucie, iż na Wschodzie z demokracją jest lepiej niż oczekiwano… co prawdopodobnie okazało się starą, sprawdzoną *ruską maskirovką*… *Mail.ru* rosyjski gigant technologiczny, którego zarząd personalnie jest mocno powiązany z Kremlem w końcu przejął aktywa *VKontakcie*, konsolidując kontrolę nad treściami w sferze informacyjnej i w socialmediach.

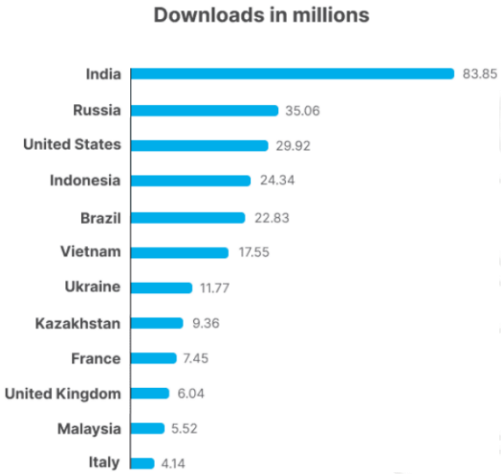
Paweł Durow Źródło: PAP / TechCrunch

Natomiast na temat wymienionego w tytule rosyjskiego komunikatora można usłyszeć wiele, w tym m.in., że dzięki osobie P. Durova jest to „*jedyny prawdziwie bezpieczny komunikator, niemożliwy do podsłuchania przez służby*". Ostatnie miesiące, ukazały szereg kontrowersji zmieniających jednak opinię wielu użytkowników na temat ww. komunikatora.

P. Durov w sierpniu br. został zatrzymany przez francuskie służby, pod zarzutem braku współpracy z organami ścigania oraz związanymi z wykorzystywaniem seksualnym nieletnich i innymi przestępstwami (w tym nielegalny handel medykamentami) dokonywanymi za pośrednictwem jego platformy. Aplikacja P. Durowa charakteryzuje się brakiem moderacji treści i polityką prywatności „oficjalnie dbającą" o zachowanie wolności słowa użytkowników, co zapewnia ogromną popularność wśród aktywistów i dysydentów będących w reżimach autorytarnych. Niestety, te same funkcje przyciągają również działalność przestępczą, w tym rozprzestrzenianie fałszywych

wiadomości, dezinformacji, propagandy, koordynację nielegalnych działań, hacktywistów, cyberprzestępców czy inne organizacje i działalności przestępcze, które w zachodnich standardach dostępne są wyłącznie w tzw. *darknecie*.

Co do samego komunikatora. Stan faktyczny jest taki, że ta popularna aplikacja bardziej przypomina serwis społecznościowy o ograniczonym szyfrowaniu, niż bezpieczne narzędzie do komunikacji. *Telegram* w przeciwieństwie do innych, bezpiecznych Zachodnich aplikacji do szyfrowanej komunikacji głosowo-tekstowej (m.in. *Signal*, *Threema*, *WhatsUp*) charakteryzuje się:



Liczba pobrań. Źródło: Statista.org

- Szyfrowaniem typu *end-to-end* wyłącznie „na żądanie" uruchomiane w ustawieniach, i ograniczeniem wyłącznie do jednego rozmówcy. W przeciwieństwie do np. *Signal'a*, który ma ww. szyfrowanie z „*default'u*" i stosuję szyfrowaną konwersację dla rozmów grupowych (do 8 os.);
- Wykorzystaniem własnego, autorskiego, zamkniętego protokołu szyfrowania *MTProto*, który nie cieszy się największym zaufaniem badaczy bezpieczeństwa i kryptologów oraz powoduje podejrzenie stosowaniem kontroli nad szyfrowanymi treściami przez władze Kremla (mimo braku oficjalnie potwierdzonych powiązań);
- Kolekcjonowaniem dużych ilości metadanych nt. użytkowników aplikacji (m.in. precyzyjną lokalizację logowania, czas, adresatów komunikacji, numery telefonów);
- Domyślne wiadomości są szyfrowane w chmurze, na serwerach *Telegram'a* umiejscowionych w… Rosji, co w związku z zamkniętym kluczem szyfrowania i niską wiarygodnością FR w zakresie przestrzegania prawa do prywatności oraz lokalną jurysdykcją pawaną, sprawia że komunikacja może podlegać masowej inwigilacji przez służby specjalne. Powyższe wpisuje się w charakter polityki wewnętrznej państwa autorytarnego. Umożliwia to również kontrolę komunikacji nie tylko wśród wewnętrznej opozycji, ale także pośród państw Rosji nieprzychylnych, jak i antyrządowych społecznościach globalnych, gdzie wiedza przez nie przetwarzana (przy liczbie użytkowników przekraczającej 900 mln), jest materiałem wywiadowczym znakomitej jakości.

***Komentarz WAC**: zalecamy usunięcie komunikatora Telegram z listy użytkowanych aplikacji. Kontrowersje związane z ww. aplikacją, ograniczone szyfrowanie, duża ilość zbieranych metadanych oraz brak przejrzystości w sferze polityki bezpieczeństwa sprawia, że opisany Telegram cechuje się niskim poziomem wiarygodności. W kontaktach prywatnych zalecamy wykorzystanie innych aplikacji cechujących się możliwym do weryfikacji otwarto-źródłowym kodem oraz pełnym szyfrowaniem typu end-to-end. Natomiast do komunikacji służbowej dla użytkowników z podmiotów publicznych zalecamy i rekomendujemy stosowanie rozwiązań dostarczanych przez Ministerstwo Cyfryzacji oraz NASK-PIB – komunikator (Threema OnPrem) oraz SKR-Z.*

Źródło: niebezpiecznik.pl

Global Security Index 2024 – Piąta edycja raportu ITU

Międzynarodowy Związek Telekomunikacyjny (ITU) opublikował piątą edycję *Global Security Index* (GSI) 2024, który jest jedną z najważniejszych analiz stanu cyberbezpieczeństwa na świecie. Raport ten ocenia gotowość państw do przeciwdziałania cyberzagrożeniom, a także ich zdolność do ochrony przed atakami, które z roku na rok stają się coraz bardziej złożone i szkodliwe

Czym jest ITU? Jest to *Międzynarodowy Związek Telekomunikacyjny* (ITU) - wyspecjalizowana agencja ONZ, której głównym celem jest rozwój technologii informacyjno-komunikacyjnych (ICT). Został założony w 1965 roku i działa na rzecz globalnej łączności, zarządzając częstotliwościami radiowymi, orbitami satelitarnymi oraz ustalając standardy telekomunikacyjne. ITU odgrywa kluczową rolę w ułatwianiu współpracy międzynarodowej w zakresie rozwoju infrastruktury telekomunikacyjnej i zmniejszaniu przepaści cyfrowej, szczególnie w krajach rozwijających się. Promuje także zrównoważoną transformację cyfrową, by zapewnić powszechny dostęp do technologii.

Ranking jest tworzony na podstawie pięciu kluczowych filarów:

1. Środki prawne (*Legal measures*): Raport analizuje istniejące krajowe ustawy i przepisy dotyczące cyberbezpieczeństwa. Wysoki poziom ochrony wymaga odpowiednich regulacji prawnych, które pozwolą skutecznie reagować na cyberzagrożenia.

2. Środki techniczne (*Technical measures*): W tej kategorii oceniane są techniczne mechanizmy ochrony, takie jak standardy bezpieczeństwa, infrastruktura oraz technologie, które umożliwiają przeciwdziałanie cyberatakom. Obejmuje to również certyfikacje systemów i rozwiązań informatycznych.

3. Środki organizacyjne (*Organizational measures*): Uwzględnia strategię cyberbezpieczeństwa na poziomie krajowym, istnienie odpowiednich instytucji oraz plany działania na wypadek cyberincydentów. Zdolność do szybkiego reagowania na zagrożenia jest kluczowa dla minimalizacji szkód.

4. Budowanie potencjału (*Capacity-development measures*): Ta kategoria koncentruje się na edukacji oraz rozwijaniu umiejętności w dziedzinie cyberbezpieczeństwa zarówno wśród profesjonalistów, jak i obywateli. Szkolenia, programy edukacyjne oraz działania promujące świadomość społeczną są tu kluczowymi elementami.

5. Współpraca (*Cooperation measures*): Cyberbezpieczeństwo wymaga współpracy na poziomie krajowym i międzynarodowym. Wymiana informacji, wspólne inicjatywy oraz koordynacja działań między krajami to istotne aspekty w walce z globalnymi zagrożeniami w sieci.

Kraje są podzielone na pięć poziomów w oparciu o ich wysiłki w zakresie cyberbezpieczeństwa, przy czym poziom 1 reprezentuje najwyższy poziom. Tak prezentuje się zestawienie państw, którym udało się uzyskać poziom 1.

Tier 1 – Role-modelling (score of 95–100)

Australia	Ghana	Morocco	Singapore
Bahrain	Greece	Netherlands (Kingdom	Slovenia
Bangladesh	Iceland	of the)	Spain
Belgium	India	Norway	Sweden
Brazil	Indonesia	Oman	Tanzania
Cyprus	Italy	Pakistan	Thailand
Denmark	Japan	Portugal	Türkiye
Egypt	Jordan	Qatar	United Arab Emirates
Estonia	Kenya	Korea (Republic of)	United Kingdom
Finland	Luxembourg	Rwanda	United States
France	Malaysia	Saudi Arabia	Viet Nam
Germany	Mauritius	Serbia	

Polska uzyskała **93,54** pkt i została zakwalifikowana do grupy państw **„*Advancing*”.**

W porównaniu do 4. edycji Raportu z 2020 roku:

- wskaźniki dla PL są wyższe w obszarach *Legal Measures* oraz *Organization Measures*.
- wskaźnik *Cooperation Measures* został utrzymany na maksymalnym poziomie 20 pkt.
- nieznaczny spadek odnotowano w punktacji dla obszarów *Technical Measures* oraz *Capacity Development* (spadek o ok. 1–1,5 pkt na 20 możliwych do przyznania).

Jak powstaje *Global Security Index*?

Ranking tworzony jest na podstawie oceny ankiety wypełnionej przez poszczególne państwa ITU. Odpowiedzi były analizowane przez grono 140 ekspertów nominowanych przez państwa członkowskie. Eksperci w 6% wywodzili się ze środowisk akademickich w 2% z organizacji obywatelskich, w 90% z przedstawicieli administracji i w 2% sektora prywatnego. Pod względem regionu skład ekspertów wyglądał następująco: 16% Afryka, 16% Ameryka, 23% Kraje arabskie, 28% Azja i Pacyfik, 3% WNP, 16% Europa, 10% Środowisko akademickie i organizacje międzynarodowe

Źródło:.itu.int

Jak oszuści wykorzystywali powódź

Tragiczne wydarzenia, takie jak powódź, są niestety często wykorzystywane przez przestępców do wyłudzania pieniędzy i danych osobowych. W ostatnich tygodniach pojawiły się liczne przypadki oszustw związanych z fałszywymi *Alertami Rządowego Centrum Bezpieczeństwa* (RCB) oraz zbiórkami charytatywnymi. Cyberprzestępcy podszywają się pod organizacje niosące pomoc, rozsyłając wiadomości SMS, e-maile oraz tworząc fałszywe strony internetowe, które mają na celu wyłudzenie danych lub przejęcie kont społecznościowych.

Jednym z oszustw było podszywanie się pod Alert RCB i rozsyłaniu fałszywych komunikatów, które zawierały linki kierujące do złośliwych stron. Wykonanie instrukcji z podstawionej strony mogło skończyć się kradzieżą pieniędzy z konta ofiary. Innym rodzajem oszustwa były strony w mediach społecznościowych zawierające szokujące informacje „Mała dziewczynka wpadła do rwącej rzeki…" – tak zaczynał się jeden z fałszywych wpisów. Próba zapoznania się z podlinkowanym materiałem, pod pretekstem weryfikacji wieku, mogła prowadzić do próby wyłudzenia loginu i hasła do konta użytkownika, co skutkowało przejęciem konta. Inne wpisy opatrzone były zdjęciem rzekomo poszkodowanej dziewczynki, przy czym w rzeczywistości obrazy były generowane za pomocą sztucznej inteligencji. Co ciekawe, posty często odnosiły się do miejscowości, które w rzeczywistości nie były objęte powodzią. W postach umieszczony był link, po próbie otwarcia strony pojawiał się komunikat w języku rosyjskim o treści: „Błąd 404 Nie znaleziono strony". Kolejne oszustwo związane było ofertą darmowych laptopów dla powodzian. Laptopy oferowała prywatna osoba z przejętych lub nowo utworzonych kont. Po nawiązaniu korespondencji, osoba zainteresowana była proszona przez oszusta, by pokryć jedynie koszty przesyłki poprzez szybką płatność w wysokości 30 - 50 zł. Jako udało się ustalić policji poszkodowanych w ten sposób było co najmniej 200 osób.

Inne wpisy przekierowywały do domeny *.rest*, która z założenia miała być wykorzystywana do promowania restauracji. Następnie użytkownikowi prezentowano rzekomy film, który po kliknięciu wywoływał monit logowania do Facebooka, pod pozorem potwierdzenia pełnoletności. Wpisane dane logowania trafiały w ręce przestępców. Inną techniką były fałszywe zbiórki pieniędzy. CBZC w swoim komunikacie poinformował, że ujawniono już ponad 200 takich nielegalnych akcji charytatywnych. Oszuści tworzyli strony internetowe i konta w mediach społecznościowych, które miały na celu zbieranie datków na rzecz rzekomo poszkodowanych. Niestety, pieniądze zamiast trafić do ofiar powodzi, trafiały na konta przestępców. Fałszywe zbiórki były prowadzone również na legalnych platformach, takich jak „*Zrzutka.pl*" czy „*Pomagam.pl*", gdzie po weryfikacji okazywało się, że ich założyciele wcale nie ucierpieli podczas powodzi, lecz wykorzystywali sytuację, podając się za poszkodowanych.

Źródła: cbzc.policja.gov.pl, www.gov.pl, cert.orange.pl

Cyberbezpieczeństwo a dezinformacja

W dyskusjach dotyczących bezpieczeństwa państwa często jednym tchem wymienia się cyberbezpieczeństwo i dezinformację, jednakże w praktyce są to dwa różne zjawiska, choć wzajemnie powiązane.

W Polsce system cyberbezpieczeństwa konstytuuje ustawa o krajowym system cyberbezpieczeństwa[1] (ustawa o KSC). Zdefiniowanie w niej cyberbezpieczeństwo obejmuje jedynie techniczne rozumienie tego pojęcia: „*odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy*" (art. 2 pkt 4). Także procedowana nowelizacja ustawy o KSC[2], która ma wdrożyć dyrektywę NIS2, pozostaje przy technicznym rozumieniu cyberbezpieczeństwa poprzez odwołanie się do definicji cyberbezpieczeństwa z unijnego aktu o cyberbezpieczeństwie: „*cyberbezpieczeństwo - oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami*".

Warto podkreślić, że Strategia Bezpieczeństwa Narodowego RP (SBN RP) z 2020 roku, stanowiąca najważniejszy drogowskaz w zakresie identyfikacji zagrożeń i wyzwań oraz interesów narodowych i środków ich realizacji, zawiera osobny rozdział dotyczący cyberbezpieczeństwa i osobny rozdział poświęcony przestrzeni informacyjnej (w którym zawarte są kwestie dezinformacji). Także rekomendacje Prezydenta RP do nowej SBN RP traktują te dwa obszary osobno, a tematyka dezinformacji ujęta jest w części dot. przestrzeni informacyjnej.

W związku z tym problematyka dezinformacji, choć również ważna, która także powinno być podejmowana przez odpowiednie instytucje, nie wpisuje się w obszar działania podmiotów KSC, których zadania i kompetencje określone są w ustawie o KSC. Podejmowanie stricte w ramach KSC tematyki dezinformacji, czy szerzej bezpieczeństwa przestrzeni informacyjnej, byłoby wyjściem poza ramy ustawowe i działaniem niespójnym z logiką i duchem zarówno obecnej ustawy o KSC, jak i jej procedowanej nowelizacji.

Przy czym warto także zauważyć, że w mediach najczęściej jest mowa o zjawisku dezinformacji, a jest to jedynie pewien wąski aspekt szerszego pojęcia, jakim jest bezpieczeństwo przestrzeni informacyjnej, w ramach którego ważnymi zagadnieniami są także komunikacja strategiczna, wojna kognitywna i operacje psychologiczne.

Jednocześnie praktyczne rozdzielenie cyberbezpieczeństwa i dezinformacji jest trudne z uwagi na wzajemne powiązania, gdyż często techniczne cyberataki wykorzystywane są w kampaniach dezinformacyjnych. Za przykład mogą posłużyć dwa głośne ataki hakerskie z tego roku: na PAP i Polską Agencję Antydopingową (POLADA). Techniczne przełamanie zabezpieczeń wykorzystano następnie do rozpowszechniania nieprawdziwych informacji, odpowiednio fałszywej depeszy prasowej oraz zmanipulowanych danych na temat polskich sportowców.

Źródła: Ustawa o krajowym systemie cyberbezpieczeństwa, Strategia Bezpieczeństwa Narodowego RP.

[1] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077)
[2] Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)

Politycy na celowniku pranksterów

Co jakiś czas ujawniane są nagrania z ważnymi politykami, w których ktoś podszywa się pod prominentnych dygnitarzy z innego państwa. Często podszywającymi się, nazywanymi pranksterami, są pracownicy rosyjskiego aparatu (dez)informacyjnego. Działania te mają na celu ośmieszyć nie tylko danego polityka, ale też dane państwo wraz z jego instytucjami, jak również wydobyć cenne informacje. Najbardziej znanymi pranksterami są dwaj Rosjanie działający pod pseudonimami Vovan i Lexus. Od 2015 r. udało im się w ten sposób podejść wielu polityków z całego świata, w tym również z Polski, m.in. premiera Wielkiej Brytanii Borisa Johnsona, premiera Kanady Justina Trudeau, premier Włoch Giorgie Meloni, prezydenta Turcji Recepa Erdoğana, prezydenta Ukrainy Petra Poroszenkę i premiera Ukrainy Arsenija Jaceniuka, a także księcia Harry'ego i Eltona Johna.

Rosyjscy pranksterzy znani jako Lexus Vovan. Źródło: Sputnik

Aby minimalizować ryzyka związane z tego rodzaju działaniami wymierzonymi w polskich polityków Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydał zalecenia, które pozwalają ustrzec się przed oszustwami polegającymi na podszywaniu się pod znane osoby.
W komunikacie na stronie Ministerstwa Cyfryzacji czytamy:

- Oficjalne rozmowy powinny być prowadzone przy użyciu zweryfikowanych kontaktów oraz środków komunikacji, zgodnie z wewnętrznymi procedurami danej instytucji, a nie za pośrednictwem prywatnych numerów, urządzeń czy kont w komunikatorach.
- Instytucje powinny wprowadzić zasady dotyczące prowadzenia rozmów między osobami na kierowniczych stanowiskach a kontaktami zewnętrznymi, szczególnie z zagranicą. Jeśli takie zasady już istnieją, warto je przejrzeć, uwzględniając rozwój technologii, które mogą umożliwiać oszustwa, takie jak tzw. *deep fake* wykorzystujący sztuczną inteligencję.
- Ważne, aby przed rozmową współpracownicy potwierdzili tożsamość drugiego rozmówcy, korzystając z oficjalnych kanałów. Warto skontaktować się telefonicznie lub mailowo z osobami, które znają drugiego rozmówcę lub z jego sekretariatem, aby upewnić się, że prośba o rozmowę jest autentyczna. Samo sprawdzenie adresu email i numeru telefonu może być niewystarczające.
- W trakcie rozmowy należy zwracać uwagę na kwestie, które mogłyby świadczyć o podszywaniu się (np. głos, słownictwo, akcent, podnoszenie kontrowersyjnych tematów, prowokacyjne pytania).
- Warto pamiętać, że czasami nie da się używać oficjalnych kanałów, na przykład podczas rozmów z osobami, które nie pełnią już publicznych funkcji. W takich przypadkach, gdy korzystamy z prywatnych numerów, urządzeń lub kont, należy szczególnie zwracać uwagę na wspomniane wcześniej sygnały, które mogą świadczyć

o oszustwie. W takiej sytuacji dobrze jest samodzielnie zweryfikować rozmówcę, kontaktując się z nim przez znane nam kanały.

- Gdy korzystamy z prywatnych numerów, urządzeń lub kont do rozmów, warto używać komunikatorów, które są otwartoźródłowe (można sprawdzić ich kod), oferują szyfrowanie end-to-end i umożliwiają weryfikację kontaktów. Dobrze, jeśli mają pozytywne opinie od organizacji zajmujących się cyberbezpieczeństwem.

Ministerstwo Cyfryzacji zwraca też uwagę, że pełne zapewnienie autentyczności rozmówców jest możliwe tylko w zamkniętych systemach komunikacyjnych. Dlatego też resort ten wprowadził bezpieczne, zamknięte środki komunikacji dla administracji publicznej i krajowego systemu cyberbezpieczeństwa - jest to Komunikator oraz SKR-Z (system do łączności niejawnej). Umożliwiają one wysyłanie wiadomości i prowadzenie połączeń głosowych. Ponadto, Ministerstwo Cyfryzacji we współpracy z NASK-PIB w ramach projektu *SecureV* prowadzi specjalistyczne, indywidualne szkolenia z zakresu cyberbezpieczeństwa dla osób pełniących kierownicze funkcje w administracji publicznej. Obejmują one m.in. aspekty związane ze świadomością cyberzagrożeń i socjotechniką stosowną przez cyberprzestępców.

Warto przy okazji wspomnieć o bardziej klasycznym rodzaju podszywania się (*spoofing*), np. pod przedstawicieli banku, wykorzystywanego przez cyberprzestępców, żeby wyłudzić od nas pieniądze, dane osobowe lub dostęp do naszych kont. Zjawisko to dzięki działaniom na gruncie krajowym zostało w ostatnim czasie znacząco ograniczone. Od 26 września 2024 r., wraz z pełnym wejściem w życie przepisów ustawy o zwalczaniu nadużyć w komunikacji elektronicznej dotyczących CLI spoofing (ang. Caller ID Spoofing), operatorzy mają obowiązek blokowania lub ukrywania sfałszowanego identyfikatora w przypadku rozpoznania CLI spoofingu. Jednak rozwiązanie to nie obejmuje połączeń międzynarodowych. Poza tym, oszuści w inny sposób poprzez socjotechnikę mogą starać oszukać swoje ofiary. Dlatego tak ważne jest zachowanie przez nas czujności i ciągłe szkolenie się z zasad higieny cyfrowej oraz cyberbezpieczeństwa.

Źródła: Ministerstwo Cyfryzacji, The Independent.

26 osób usłyszało 224 zarzuty karne za kierowanie i udział w grupie przestępczej, pranie pieniędzy i oszustwa!

Białostoccy funkcjonariusze CBZC działając pod nadzorem Prokuratury Okręgowej w Łomży, rozbili dwie zorganizowane grupy przestępcze. Jedna zajmowała się udostępnianiem cyberprzestępcom z całej Polski infrastruktury informatycznej, umożliwiającej dokonywanie oszustw przez podsyłanie linków do fałszywych ogłoszeń sprzedaży sprzętu elektronicznego (*scam*). Druga oszukiwała, wysyłając wiadomości od rzekomych członków rodziny z prośbą o zapłatę zaległych rachunków.

Policjanci z CBZC w Białymstoku podczas wielomiesięcznego śledztwa przeanalizowali znaczne ilości zgromadzonych danych, w tym przepływów finansowych dotyczących portfeli kryptowalutowych, co pozwoliło na wykrycie i namierzenie sprawców, a następnie zatrzymanie łącznie 26 osób, w tym osób kierujących całym procederem i zajmujących się m.in. praniem pieniędzy. Sprawcy za pośrednictwem popularnych platform kontaktowali się z pokrzywdzonymi, tworzyli fikcyjne ogłoszenia sprzedaży telefonów komórkowych, sprzętu elektronicznego i innych przedmiotów w okazyjnych cenach, a następnie wysyłali spreparowane linki przekierowujące na fałszywe portale sprzedażowe oraz bramki płatnicze i wyłudzali płatności BLIK.

Cyberprzestępcy specjalizowali się również w pozyskiwaniu nielegalnych dochodów poprzez wysyłanie wiadomości do pokrzywdzonych z prośbą o pilną zapłatę zaległych rachunków, podając się za ich „córkę" lub „syna". Pieniądze trafiały na konta bankowe założone na „słupów", a następnie były transferowane na inne konta, portfele kryptowalutowe lub wypłacane z bankomatów przez tzw. wybieraków. Sprawcy wykorzystywali specjalne oprogramowanie umożliwiające prowadzenie kampanii SMS-owej, dzięki której mogli dotrzeć do kilkudziesięciu tysięcy osób w Polsce i za granicą.

W wyniku działań cyberprzestępców obydwu grup, oszukanych mogło zostać wiele tysięcy osób, a straty szacuje się w milionach złotych.

Funkcjonariusze ustalili skład poszczególnych grup oraz role, jakie pełnili ich członkowie. Zabezpieczyli i zablokowali także infrastrukturę informatyczną służącą do cyberprzestępczej działalności, uniemożliwiając jej dalsze użytkowanie. W toku postępowania zabezpieczono też serwer udostępniany w ramach hostingu „*bulletproof*" z dziesiątkami terabajtów danych, liczny sprzęt komputerowy, telefony komórkowe, elektroniczne nośniki danych, a także kryptowaluty. Podejrzani usłyszeli łącznie 224 zarzuty karne, w tym za kierowanie i udział w grupie przestępczej, pranie pieniędzy i oszustwa internetowe. Tego typu przestępstwa są zagrożone karą nawet do 10 lat pozbawienia wolności. Decyzją sądu aresztowano do tej pory 16 osób, a dwóch nieletnich sprawców umieszczono w schronisku dla nieletnich.

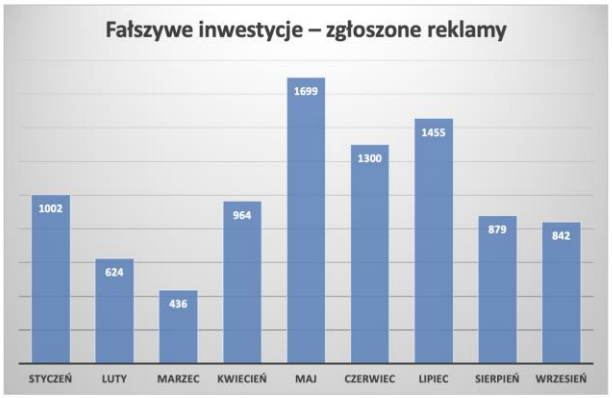
Postępowanie od początku nadzorowane jest przez Departament do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej. Ma ono charakter rozwojowy i obejmuje swoim zasięgiem nie tylko Polskę.

https://cbzc.policja.gov.pl/bzc/aktualnosci/409,26-osob-uslyszalo-224-zarzuty-karne-za-kierowanie-i-udzial-w-grupie-przestepczej.html

Podsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta

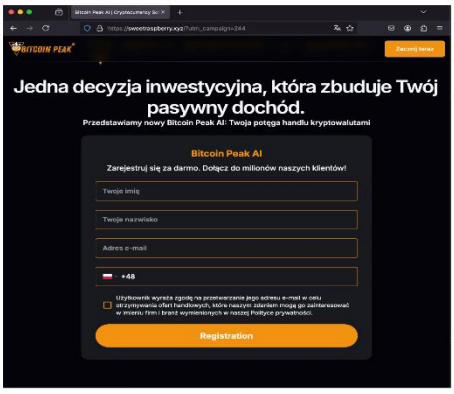
We wrześniu 2024 roku CSIRT KNF wykrył i zgłosił do zablokowania 2 852 domen, które wcześniej zakwalifikowane zostały jako wyłudzające dane (m.in. loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe), dla porównania CERT Polska dodał na listę ostrzeżeń 6 211 domen. A na koniec omawianego miesiąca, na liście hole znajdowało się 238 207 domen.

W związku ze znaczącą liczbą fałszywych reklam publikowanych na platformie Facebook promujących rzekomą możliwość inwestowania, a w rzeczywistości powodujące wysokie straty finansowe u klientów banków, CSIRT KNF wypracował mechanizmy wykrywające takie działanie przestępcze oraz procesy przekazywania fałszywych reklam do blokady. Wykres przedstawia wykryte i zgłoszone do blokady reklamy fałszywych inwestycji na portalu społecznościowym Facebook, w podziale na kategorie wykorzystywanego wizerunku.

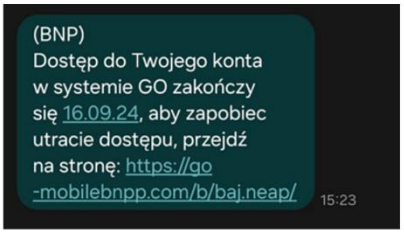


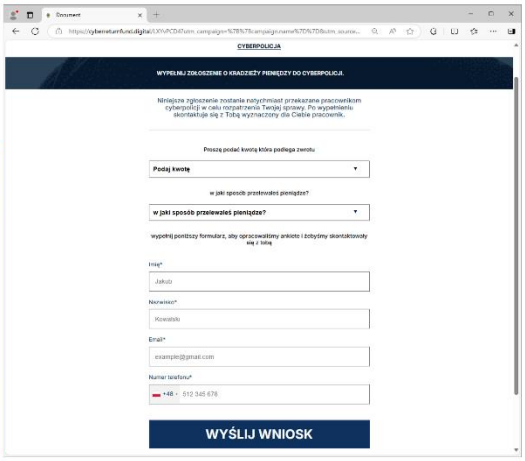
Zdarza się również, że sposobem na wzmocnienie prowadzanej gry psychologicznej, jest wykorzystanie wizerunku znanych instytucji. We wrześniu 2024 roku obserwowaliśmy kampanie podszywające się m.in. pod Bank Peako, Narodowy Bank Polski, czy Komisję Nadzoru Finansowego.

Powtarzającym się schematem jest również 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.



Zidentyfikowaliśmy również kampanie przestępcze podszywające się bezpośrednio pod podmioty z sektora finansowego. Przestępcy wykorzystują 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. Przestępcy podszywali się pod Bank BNP Paribas oraz Bank Pekao publikowali reklamy na platformie Facebook oraz wysyłali wiadomości SMS. Informowali w nich o rzekomej możliwości otrzymania dodatkowych 3% do lokaty i/lub informowali o rzekomym wygaśnięciu dostępu do bankowości elektronicznej. W rzeczywistości linki prowadziły do stron *phishingowych*, łudząco przypominających prawdziwe strony.





Cyberprzestępcy wykorzystywali również trudna sytuację w Polsce i publikowali reklamy informujące o rzekomej zbiórce na pomoc osobom dotkniętym powodzią. Jeżeli ktoś uwierzył w zbiórkę i chcąc pomóc, kliknął w link, trafił na stronę, która nielegalnie wykorzystywała wizerunek Wielkiej Orkiestry Świątecznej Pomocy. W rzeczywistości przestępcy wyłudzali w ten sposób dane kart płatniczych.

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.

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.