Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

04/2024

SPIS TREŚCI

Zmiana rodzaju aktywności chińskich grup APT wspieranych przez państwo (state-sponsored)

Ostatnie lata charakteryzują się zmianą układu sił w ramach relacji międzynarodowych i geografii politycznej. Ostatnie trzy dekady po upadku Związku Sowieckiego cechowały się monocentryczną dominacją technologiczną i gospodarczą Stanów Zjednoczonych. Jednakże, chiński nowy „Długi Marsz" po doścignięciu USA w zakresie PKB, został przekierowany z masowej, prostej produkcji przemysłowej - na wyścig w zakresach zaawansowanych technologii w obszarach m. in. robotyki, nanotechnologii, IT, biotechnologii, AI czy łączności.

Te ostatnie, uznawane są za kluczowe dla rozwoju Państwa Środka. Wykładniczy wzrost potencjału w zakresie technologii cyfrowych, umożliwiony został w dużej mierze poprzez szpiegostwo przemysłowe i kradzież własności intelektualnej, które w okresie minionych dwóch dekad były możliwe dzięki zaawansowaniu... technologicznemu chińskich hakerów. Obecne „uczenie" się od innych, a uprzednie kopiowanie całych rozwiązań technicznych pozyskiwanych z krajów Zachodu stanowiło do niedawna *clue* rozwoju chińskich technologii. Jednak okres od 2018 r. i głośnego wystąpienia Xi Jinpinga dotyczącego *„nowej ideologii na nową erę"*, zmienił wartościowanie potencjału Chińskiej Republiki Ludowej (ChRL) i dążenie do jakościowej transformacji Chin. Współcześnie Państwo Środka zaadoptowało się do warunków światowej gospodarki cyfrowej. Rozwiązania projektowane i produkowane w Shenzhen znajdują się praktycznie w każdym urządzeniu elektronicznym na świecie, a firmy jak *Tencet* dołączyły do pierwszej dziesiątki największych firm technologicznych globu (obok m.in. *Apple*, *Intela*, czy *Microsoftu*).

Źródło: *bankinfosecurity.com*

Jednakże autorytarna charakterystyka chińskiego ustroju publicznego oraz lokalne kultura i podejście do „własności", zgoła odmienne od tych, cechujących cywilizację Zachodu, stanowi wzrastające niebezpieczeństwo dla państw „Bogatej Północy". Wysoka efektywność działań aktywnych w cyberprzestrzeni w pozyskiwaniu intratnych danych wrażliwych powoduje wzrost zagrożeń związanych z chińską aktywnością, potęgowaną niejawnym wsparciem państwa chińskiego udzielanego lokalnym grupom APT. Dotychczas zespoły hakerów z ChRL w przeciwieństwie do podmiotów rosyjskich czy irańskich, nie były skupione na możliwościach kinetycznego wpływu czy pozyskiwaniu danych wywiadowczych o znaczeniu obronnym, a koncentrowały się przede wszystkim na szpiegostwie przemysłowym, technologicznym i kradzieży danych wrażliwych.

Zgodnie z opublikowanym raportem przez ***CISA,*** grupy hakierskie wspierane przez ChRL, dalej stanowią największe zagrożenie dla bezpieczeństwa sektorów publicznego i prywatnego USA. Jednak zmieniły one swoje *modus operandi.* Ewaluowały z działalności szpiegowskiej, na trwałą infiltrację sieci oraz uśpienie tej aktywności, celem późniejszego wybudzenia i potencjalnego prowadzenia destrukcyjnej działalności o skutkach kinetycznych w świecie rzeczywistym. Wyraźnym celem chińskich ataków stały się małe i lokalne podmioty gospodarcze, będące jednak kluczowymi dla bezpieczeństwa i stabilności wewnętrznej USA elementami infrastruktury krytycznej.

Federacja Rosyjska (FR) utrzymuje wysoką aktywność swoich grup APT

Trwająca od 2014 r. wojna na Ukrainie i jej brutalna eskalacja w 2022 r. w przeciwieństwie do innych konfliktów zbrojnych „ery cyfrowej", cechuje się szerokim wykorzystaniem cyberprzestrzeni w prowadzeniu działań zbrojnych oraz realizacji *spectrum* działań wspierających np. w sferze informacyjnej. Obserwacja przestrzeni cyfrowej szczególnie ostatnich dwóch lat umożliwia dostrzeżenie ewolucyjnych zmian rozwojowych w tej domenie walk. Obecne napięcia geopolityczne w wielu regionach świata uwypuklają sojusze cyfrowe oraz wspólnoty interesów grup hakierskich i haktywistycznych, których aktywność jest zbieżna z sojuszami politycznymi i celami państw będących obecnie pariasami międzynarodowych stosunków politycznych (m.in. Rosja, Iran, Korea Północna, Palestyna/Liban).

Źródło: *cisa.gov*

Częstokroć definiowanie atrybucji grup *Advanced Peresistent Threats/APT* polega na rozpatrywaniu wskaźników kompromitacji (*IoC's*), wraz z analizą kontekstową wydarzeń w sferze informacyjnej, medialnej czy politycznej. Ze względu na stosowanie przez hakerów zaawansowanych technik i narzędzi anonimizacji oraz metod i procedur bezpieczeństwa (tzw. *opsec*), korelacja IoC'ików ze zdarzeniami w świecie rzeczywistym oraz z historycznie przypisanymi do danych grup APT atakami (ich charakterystyką na podstawie *tactics, techniques, and procedures/TTP's*), jest jedną z najefektywniejszych metod pracy analitycznej zespołów bezpieczeństwa *Cyber Threat Intelligence/CTI*.

Na tej podstawie analitycy CTI stwierdzają, utrzymujące się od początku eskalacji wojny na Ukrainie bardzo wysokie zaangażowanie podmiotów w cyberprzestrzeni związanych z FR. Pierwsza połowa maja, cechuje się wysypem specjalistycznych opracowań alarmujących o cyfrowej działalności prorosyjskiej. M.in. Firma *NETSCOUT* informuje, o dotychczas niespotykanej skali ataków typu *DDoS* prowadzonych przez grupy haktywistyczne (*NoName057*) na mołdawską administrację państwową i podmioty publiczne. Firma *CheckPoint* przekazuje informacje nt. działalności rosyjskiej grupy ransomware *LockBit*. *Microsoft* publikuje raport o zdefiniowaniu nowego narzędzia i metodologii ataków grupy STRONTIUM/APT28. Czy w końcu zaobserwowana przez polskie zespoły CSIRT NASK i CSIRT MON kampania związana z rosyjskim GRU i grupą APT28 prowadzącą ataki wymierzone w polskie instytucje rządowe.

Powyższe linki są tylko ułamkiem informacji dotyczącej działalności grup powiązanych z FR w ostatnim czasie. W pierwszym okresie eskalacji z 2022 r. specjaliści od bezpieczeństwa militarnego i analitycy CTI, byli zaskoczeni niską aktywnością rosyjskich działań w cyberprzestrzeni, zapewne spodziewając się dużych i głośnych operacji o kinetycznych skutkach. Obecnie można stwierdzić, że działalność FR ewaluowała. Głośne medialnie ataki, mimo stosunkowo niskiej szkodliwości (*ransomware/DDoS*) są prowadzone przez grupy działające w „ciemnej" sferze publicznej, jak haktywiści czy gangi ransomware. Natomiast bezpośrednio sterowane przez służby specjalne grupy, jak APT28 i APT29 koncentrują się na cichych i długoterminowych operacjach wobec podmiotów wrażliwych.

Koalicja na rzecz wsparcia Sił Zbrojnych Ukrainy

W lutym br. 11 państw podpisało porozumienie o współpracy w ramach Koalicji IT na rzecz wsparcia wysiłku obronnego Ukrainy. Uczestnikami Koalicji IT są Estonia i Luksemburg jako wiodące kraje, a także Belgia, Dania, Islandia, Włochy, Łotwa, Litwa, Holandia, Wielka Brytania i sama Ukraina. Ponadto 7 państw ma status obserwatora. Koalicja IT to specjalna grupa państw w ramach *Grupy Kontaktowej ds. Obrony Ukrainy* ("format Ramstein") działająca w zakresie IT, łączności i cyberbezpieczeństwa. W sumie powołano 8 tego rodzaju koalicji, np. w zakresie zdolności lotniczych, obrony przeciwlotniczej i przeciwrakietowej.

Celem Koalicji IT jest udzielenie pomocy Ukrainie w ciągu najbliższych 6 lat w celu budowy odpornej i interoperacyjnej infrastruktury informatycznej *Ministerstwa Obrony i Sił Obronnych Ukrainy*. Koalicja IT służy też wymianie doświadczeń w zakresie wykorzystania innowacyjnych technologii i realizacji wspólnych projektów. W kwietniu członkowie Koalicji IT ustalili mapę drogową mającą na celu ustalenia wkładów poszczególnych państw oraz zaplanowanie zamówień zaspokajających krytyczne potrzeby ukraińskiego wojska pomagające wzmocnić przewagę technologiczną Ukrainy na polu bitwy. Podkreślono także otwarcie na dołączenie kolejnych krajów.

Dostawa sprzętu dla Sił Zbrojnych Ukrainy w ramach Koalicji IT. Źródło: Ministerstwo Obrony Ukrainy

Na przełomie kwietnia i maja dostarczono już pierwsze dostawy sprzętu dla *Sił Zbrojnych Ukrainy*. Laptopy, monitory i inny sprzęt komunikacyjny o wartości 900 tys. EUR mają być niezwłocznie przekazane jednostek wojskowych. Przekazany sprzęt usprawni komunikację i planowanie zadań na poziomie taktycznym. Łączność to jeden z priorytetów ukraińskiej armii. Sprawne i szybkie zakupy odbyły się dzięki *Agencji Wsparcia i Zamówień NATO* (NSPA). W ramach koalicji IT udało się już zebrać wkład finansowy i rzeczowy w wysokości ponad 36 mln euro. Wkłady w kwocie ponad 23 mln euro nadal nie zostały wniesione.

Koalicja IT to format współpracy z udziałem resortów obrony. Natomiast polskie M*inisterstwo Cyfryzacji* uczestniczy w innych inicjatywach wspierających cyberbezpieczeństwo Ukrainy. Polska dostarczyła wschodniemu sąsiadowi największą liczbę terminali *Starlink*, bo ponad 20 tys. Sprzęt ten zapewnia wsparcie nie tylko dla armii, ale także dla szpitali, infrastruktury krytycznej i utrzymania stałego dostępu do Internetu szerokopasmowego dla cywilów. Polska przekazała także ponad 500 magazynów energii typu *Powerwall*, które wspierają zarówno wojsko, jak i sektor cywilny.

Nasze *Ministerstwo Cyfryzacji* bierze też udział w *Mechanizmie Tallińskim*. Jest to grupa państw sojuszniczych w ramach NATO, która ma na celu koordynację i wzajemne wspieranie działań poprawiających cyberbezpieczeństwo Ukrainy oraz budowanie jej odporności na cyberzagrożenia. W ramach tej inicjatywy Polska pełni rolę tzw. *Back Office* zbierającego

zapotrzebowanie strony ukraińskiej w zakresie cyberbezpieczeństwa z jednej strony, a z drugiej oferty konkretnej pomocy i wsparcia od członków grupy.

W trakcie majowej wizyty w Kijowie Wicepremier i Minister Cyfryzacji, Krzysztof Gawkowski, podpisał z ukraińskim Wicepremierem i Ministrem Transformacji Cyfrowej, Mychajło Fedorowem, *Memorandum Cyfrowe*, które ma na celu wzmocnienie wzajemnych relacji w zakresie cyberbezpieczeństwa i usług cyfrowych. W trakcie wizyty omówiono także rozwój aplikacji *Dija* i *mObywatel*. W obu krajach są to bardzo popularne aplikacje dające dostęp do wielu cyfrowych usług publicznych. Celem partnerstwa Polski i Ukrainy jest też współpraca w dziedzinie technologii cyfrowych i innowacji, rozwój branży IT, sztucznej inteligencji, e - administracja.

Minister obrony Ukrainy ogłasza utworzenie koalicji IT na spotkaniu w Ramstein
Źródło: *pravda.com.ua*

Jak wskazał minister Fedorow: *„Polska jest jednym z kluczowych partnerów Ukrainy. Od początku inwazji na pełną skalę kraj ten wspierał nasze cyfrowe państwo na poziomie strategicznym. W szczególności zapewnił infrastrukturę do hostowania ukraińskich rejestrów, dzięki czemu urząd skarbowy kontynuował pracę, a Ukraińcy mają dostęp do usług elektronicznych”*. Jak w swym komunikacie napisało Ministerstwo Transformacji Cyfrowej Ukrainy: *„w szczególności w Polsce znajduje się centrum danych Państwowej Służby Podatkowej Ukrainy, które Polska zbudowała na preferencyjnych warunkach. A także zapasowe centrum danych do przechowywania systemów Ministerstwa Sprawiedliwości Ukrainy, w którym przechowywane są ważne systemy”*.

Źródła: *mil.gov.ua, thedigital.gov.ua, gov.pl/cyfryzacja*

Współpraca chińsko-rosyjska kwitnie na wielu różnych płaszczyznach w tym w zakresie szyfrowanej komunikacji kwantowej

Poziom partnerstwa rosyjsko-chińskiego w domenach dyplomatycznej, informacyjnej, wojskowej, gospodarczej i cyber rośnie. Według przywódców obu krajów, strategiczne partnerstwo Chin (ChRL) i Rosji (FR) ma na celu "przeciwdziałanie dominacji USA" i zapoczątkowanie "wielobiegunowego porządku światowego".

Mozi, chiński satelita wykorzystany w tym teście. (Źródło zdjęcia: Chińska Akademia Nauk)

W kwietniu 2024 r. ChRL i FR kontynuowały zacieśnianie strategicznej współpracy w ramach DIMEC (*diplomatic*, *informational*, *military*, *economic*, *cyber*). W zakresie informacyjnym oba narody wyraziły wspólny pogląd, że działania Stanów Zjednoczonych w Europie i na Indo-Pacyfiku destabilizują bezpieczeństwo regionalne. Pod względem wojskowym Chiny i Rosja podpisały umowy o współpracy w zakresie morskich misji ratunkowych, ale powtórzyły, że współpraca wojskowa Pekinu i Moskwy nie jest skierowana przeciwko żadnemu "*państwu trzeciemu*". FR nadal zwiększa handel międzynarodowy z ChRL, podczas gdy napięcia geopolityczne z Zachodem stopniowo eskalują w związku z wojną Rosji przeciwko Ukrainie.

Co ciekawe w domenie cyber, **FR poinformowała o wspólnym chińsko-rosyjskim, pierwszym w historii teście szyfrowanej komunikacji kwantowej, który miał miejsce pod koniec 2023 r.** Według wyników badań przeprowadzonych przez rosyjski *Narodowy Uniwersytet Nauki Technologii* NUST MISIS, oba kraje przeprowadziły udane eksperymenty w zakresie przesyłania zaszyfrowanych wiadomości kwantowych za pośrednictwem chińskiego satelity komunikacji kwantowej *Mo Zi* (墨子). Współpraca ta, z początku 2019 r., stanowi element rosyjskiego programu "*Priorytet 2030*" i ma na celu ulepszenie technologii ochrony danych. Test został przeprowadzony przy użyciu satelity ze stacji naziemnej w pobliżu Moskwy w Rosji do innej stacji znajdującej się w pobliżu Urumqi w Chinach, ponad 3800 kilometrów, według *South China Morning Post*. Satelita wykorzystany do osiągnięcia kwantowej komunikacji, Mozi (zwany Micius), znajduje się na orbicie od 2016 r. i jest zarządzany głównie przez *Chińską Akademię Nauk*. Współpraca z rosyjskimi naukowcami rozpoczęła się w 2020 r. Chociaż szczegóły dotyczące wymiany informacji między FR, a ChRL pozostają nieujawnione, wyniki ich współpracy najpewniej będą wspierać transfer niejawnych informacji rządowych.

Komunikacja kwantowa jest - przynajmniej w teorii - najbezpieczniejszą możliwą formą transmisji danych, wykorzystującą mechanikę kwantową, głównymi wadami jednak są ograniczone zastosowanie/rozwój obliczeń kwantowych i fundamentalne słabości zasięgu w obecnych technologiach transmisji. Podczas gdy technologia ta stale się rozwija, wydaje się, że minie jeszcze trochę czasu, zanim zostanie wykorzystana na dużą skalę. Alexey Fedorov z *rosyjskiego NUST* oraz *Rosyjskiego Centrum Kwantowego* stwierdza: "Kwantowe sieci komunikacyjne mogą mieć wiele zastosowań, ale na razie systemy kwantowe idealnie nadają się do badań naukowych". Podkreślił też zainteresowanie rosyjskiego sektora finansowego obliczeniami kwantowymi, a nawet nawiązał do możliwości stworzenia w przyszłości **kwantowej sieci komunikacyjnej między krajami BRICS.**

Źródło: tbsnews.net, tomshardware.com, RecordedFuture.com, .iotworldtoday.com

Europa w obliczu rosnących zagrożeń w cyberprzestrzeni - zbliżające się wybory do Parlamentu Europejskiego

Unia Europejska wszczęła w ostatnim czasie dochodzenie w sprawie firmy *Meta* w związku z podejrzeniem nieprzestrzegania nowych zasad uczciwości wyborczej, wprowadzonych przed czerwcowymi wyborami do *Parlamentu Europejskiego*. ***Komisja Europejska*** **opublikowała w marcu szereg zasad, których muszą przestrzegać największe platformy technologiczne w ramach ustawy o usługach cyfrowych. Zasady te wymagają od firm wdrożenia procesów mających na celu zwalczanie operacji wywierania wpływu, szczególnie w przypadku wrażliwych wydarzeń politycznych, takich jak wybory.** Ogłaszając formalne postępowanie przeciwko *Meta*, przewodnicząca Komisji Ursula von der Leyen powiedziała: "Ta Komisja stworzyła środki mające na celu ochronę europejskich obywateli przed ukierunkowaną dezinformacją i manipulacją ze strony państw trzecich. Jeśli podejrzewamy naruszenie zasad, działamy". Dochodzenie w sprawie *Meta* jest następstwem ostrzeżenia wiceprzewodniczącego *Komisji Europejskiej* Margaritisa Schinasa, że rosyjska ingerencja w wybory "zagraża funkcjonowaniu naszego społeczeństwa i bezpośrednio podważa nasz demokratyczny etos".

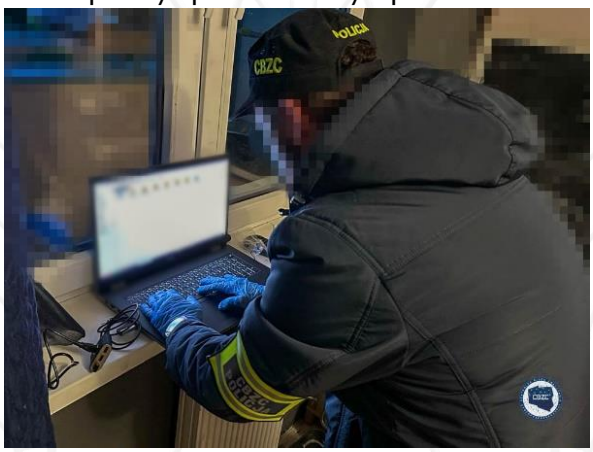
Budynek Parlamentu Europejskiego.

Ponadto należy mieć na uwadze, że rok 2024 trzeba bez wątpienia zaliczyć do 'roku wyborów' z uwagi na to, że wypadają one w wielu krajach UE. W obliczu rosnących zagrożeń, niemieckie *Federalne Ministerstwo Spraw Wewnętrznych i Społeczności* na stronie internetowej wydało artykuł: „Ochrona wyborów europejskich przed zagrożeniami hybrydowymi, w tym dezinformacją: Rozpoznawanie zagrożeń hybrydowych, wykrywanie kampanii dezinformacyjnych, podejmowanie działań w celu zapewnienia bezpieczeństwa wyborów". Dodatkowo polskie Ministerstwo Spraw Zagranicznych wydało niedawno oświadczenie w sprawie szkodliwych działań Federacji Rosyjskiej w cyberprzestrzeni wyrażając pełną solidarność z Niemcami i Czechami w związku z wrogą kampanią prowadzoną przeciwko ich partiom politycznym i instytucjom demokratycznym. Powyższe działania świadczą o podwyższonym stanie gotowości poszczególnych krajów w zakresie bezpieczeństwa cyberprzestrzeni, ale także rosnącej świadomości zagrożeń, zwłaszcza w obliczu kolejnego ważnego wydarzenia jakim są zbliżające się wybory do *Parlamentu Europejskiego*.

Źródła: therecord.media, bmi.bund.de

Operacja DAKOTA – uderzenie w przestępczość o charakterze pedofilskim

Policjanci *Centralnego Biura Zwalczania Cyberprzestępczości* kolejny raz uderzyli w sprawców przestępstw o charakterze pedofilskim. Funkcjonariusze zarządów i wydziałów CBZC z całej Polski zatrzymali 66 osób, spośród których 62 przedstawiono zarzuty karne posiadania, udostępniania w sieci i produkcję materiałów przedstawiających seksualne wykorzystanie małoletnich. Policjanci w wyniku 103 przeszukań zabezpieczyli ponad 166 tys. plików z nielegalnymi treściami.



Materiał własny CBZC

Walka z seksualnym wykorzystaniem osób małoletnich i przeciwdziałanie udostępnianiu materiałów przedstawiających takie wykorzystanie w Internecie, jest jednym z zadań policjantów *Centralnego Biura Zwalczania Cyberprzestępczości*. W ostatnim tygodniu funkcjonariusze kolejny raz uderzyli w sprawców przestępstw, o charakterze seksualnym przeprowadzając na terenie całego kraju operację „*Dakota*".

359 funkcjonariuszy biorących udział w operacji, zatrzymało łącznie 66 osób w wieku od 19 do 72 lat, spośród których 62 osoby podejrzane są o posiadanie, udostępnianie w Internecie i produkcję materiałów przedstawiających seksualne wykorzystanie osób małoletnich. Policjanci przeprowadzili 103 przeszukania, w trakcie których ujawnili i zabezpieczyli ponad 166 tys. plików z nielegalnymi treściami, zabezpieczając łącznie 1280 różnego rodzaju nośników danych w tym komputerów i telefonów. Wśród zabezpieczonych materiałów znajdują się pliki, przedstawiające drastyczne przypadki wykorzystywania dzieci nawet w wielu niemowlęcym.

Materiał własny CBZC

W ramach prowadzonej operacji współpracowaliśmy z amerykańskimi (FBI) i brytyjskimi (NCA) służbami. W wyniku tych działań ustalono mężczyznę, który produkował materiały o pedofilskim charakterze z udziałem swojej kilkuletniej córki oraz innego mężczyznę, który w dwóch przypadkach wytwarzał takie materiały z udziałem kilkuletnich dzieci pozostających z nim w bliskich relacjach.

Kolejna ustalona osoba, pomagała przeprowadzać remonty mieszkań u rodzin, od wielu lat znanych mężczyźnie, dzięki czemu miał możliwość ukrywania kamery w łazience i nagrywania osób małoletnich. Jeszcze inny wyszukiwał na portalach społecznościowych zdjęcia małoletnich dziewcząt, robione z ukrycia, i podając się za kobietę, nawiązywał z nimi kontakt on-line, szantażując je do wysyłania kolejnych obscenicznych materiałów. Na tę chwilę ujawniono trzy ofiary tego mężczyzny.

To kilka najbardziej drastycznych przykładów ujawnionych w trakcie prowadzonej operacji. Wszystkie te osoby usłyszały zarzuty karne przeciwko wolności seksualnej i obyczajności. Decyzją sądów 25 podejrzanych zostało tymczasowo aresztowanych.

Cała operacja była ściśle koordynowana z *Departamentem ds. Cyberprzestępczości i Informatyzacji Prokuratury Krajowej*, a także prokuraturami w całym kraju. Współpraca odbywała się również na poziomie międzynarodowym m.in. z EUROPOL-em i amerykańską organizacją walczącą z tego rodzaju nadużyciami NCMEC (*National Center for Missing and Exploited Children*).

Materiał własny CBZC

W przeprowadzenie operacji DAKOTA, zaangażowani zostali funkcjonariusze posiadający odpowiednie przygotowanie merytoryczne oraz psychologiczne, pozwalające na pracę z bardzo obciążającym materiałem dowodowym. Opisywana operacja o szerokiej skali działań analitycznych i operacyjnych to duże wyzwanie i odpowiedzialność w podejmowaniu decyzji. Warto tutaj zaznaczyć, że jest to już czwarta taka operacja Biura, a łącznie zatrzymano już 223 osoby, z czego 88 zostało tymczasowo aresztowanych. W wyniku przeprowadzonych 378 przeszukań zabezpieczono niemal 700 tys. plików z nielegalnymi treściami.

Teraz przed śledczymi żmudna i niezwykle czasochłonna praca z setkami tysięcy zabezpieczonych plików. Praca niezwykle obciążająca, z uwagi na drastyczne treści zawarte na zdjęciach i filmach o charakterze pedofilskim. W wyniku tej analizy będą podejmowane dalsze decyzje co do przedstawiania podejrzanym kolejnych zarzutów karnych i ewentualnego zatrzymania kolejnych osób.

Ze względu na szczególny charakter ujawnionych przestępstw, i mając na uwadze ochronę ofiar przed wtórną wiktymizacją, nie udzielamy bliższych informacji.

Więcej informacji nt. operacji pod linkiem:

Operacja DAKOTA – uderzenie w przestępczość o charakterze pedofilskim - Aktualności - Centralne Biuro Zwalczania Cyberprzestępczości (policja.gov.pl)

Cyberpodsumowanie miesiąca CSIRT KNF – Ochrona klienta

W kwietniu 2024 roku CSIRT KNF wykrył i zgłosił do zablokowania 7 167 domen (w styczniu 6 249 domeny), które wcześniej zakwalifikowane zostały jako wyłudzające dane (loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody *BLIK* i/lub dane osobowe, etc.). Dodatkowo, w kwietniu 2024 roku analitycy CSIRT KNF zgłosili również do blokady 321 fałszywych profili, które publikowały fałszywe reklamy inwestycyjne.

W minionym miesiącu przestępcy nieustannie stosowali, znany pod nazwą „*fraud inwestycyjny*", schemat działania. W ramach niego podszywali się pod znane osoby oraz instytucje, celem nakłonienia potencjalne ofiary do rzekomego zainwestowania środków i otrzymania wysokiej stopy zwrotu. W rzeczywistości prowadzili grę psychologiczną, mającą na celu narażanie ofiary na wysokie starty finansowe. Przestępcy nadal chętnie wykorzystują technologię *deepfake* do tworzenia materiałów oszukańczych. Wykorzystują wizerunki znanych osób, generując nagrania video na których przedstawiona jest treść zachęcająca do rzekomych inwestycji.

W kwietniu 2024 roku zauważyliśmy, że przestępcy nakładają na nagrania modyfikacje graficzne. Działanie to może wynikać z chęci ukrycia nagrań przed detektorami implementowanymi na portalach społecznościowych.

Z materiałem tym zapoznać można się z nim pod adresem: *https://cebrf.knf.gov.pl/deepfake.*

Skoro przestępcy wykorzystują wizerunek znanych instytucji, aby zwiększać wiarygodność kampanii phishingowych, to również chętnie podszywają się pod polskie Banki. Tego typu kampanie obserwowane są przez nas regularnie. Atakujący wyłudzają w ten sposób informacje o kartach płatniczych oraz dane uwierzytelniające do bankowości elektronicznej, jak i zachęcają do pobierania złośliwych aplikacji. W kwietniu 2024 roku przestępcy nadal wykorzystywali ten sposób działania. Tym razem publikowali reklamy na platformie *Facebook* oraz wysyłali wiadomości *iMessage* (funkcjonalność komunikatora opracowanego przez firmę *Apple*). Wiadomości *iMessage* wykorzystywali również podszywając się pod *Pocztę Polską*. W wiadomościach informowali o rzekomej konieczności aktualizacji adresu. Podobna kampania phishingowa, wykorzystująca wizerunek *Poczty Polskiej*, miała już kilkukrotnie miejsce w latach 2023 i 2024. Równie regularnie jak pod banki, przestępcy podszywali się również pod firmy kurierskie, tym razem wykorzystywali wizerunek firmy *InPost*. Informowali o rzekomej konieczności uzupełnienia adresu dostawy. Tym sposobem zachęcali do kliknięcia w link, który w rzeczywistości prowadził do strony phishingowej. Także w ten sposób oszuści

chcieli pozyskać informację o danych kart płatniczych. Poprzez wiadomości e-mail oszuści podszywali się pod Allegro, informując o rzekomy zawieszeniu konta. Odblokowanie konta wymagało aktualizacji danych transakcyjnych, którego dokonać można poprzez kliknięcie w „*AKTUALIZUJE SWOJE DANE*”. Kolejną kampanię phishingową, jaką przygotowali przestępcy wykorzystywała wizerunek NFZ. Informowali o rzekomej możliwości wyrobienia sobie nowej karty, która „aktualizuje uprawnienia oraz gwarantuje skuteczniejsze pokrycie kosztów opieki zdrowotnej”. W rzeczywistości przestępcy wyłudzali dane kart płatniczych oraz dane osobowe. Podobnie jak w minionych miesiącach nie zabrakło podszyć pod platformy streamingowe, które dystrybuowane były poprzez wiadomości e-mail oraz SMS, a także reklam na platformie *Facebook* w której oferowali rzekomą możliwość odebrania za darmo gry *Rust*. Celem finalizacji operacji zachęcali do kliknięcia w linku, a następnie wyłudzali dane logowania do platformy *Steam*.

Screen scamu internetowego.
Źródło: cebrf.knf.gov.pl

Ponownie zachęcamy również do lektury naszego raportu rocznego, w którym prezentujemy podsumowanie cyberzagrożeń dla rynku finansowego w 2023 z perspektywy CSIRT KNF. W opracowaniu znajdują się m.in. statystyki z naszych działań, najczęściej spotykane cyberoszustwa oraz prognozy na rok 2024. Raport dostępny jest tutaj: *https://cebrf.knf.gov.pl/images/Raport_roczny_CSIRT_KNF.pdf*

„*Wiedza to potęga*”, dlatego (jak zawsze) zachęcamy także do śledzenia informacji o bieżących schematach i scenariuszach przestępczych na naszych profilach w mediach społecznościowych: *X (Twitter)*, *LinkedIn* oraz *Facebook* oraz na stronie internetowej *UKNF: 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

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*