Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

05/2024

SPIS TREŚCI

Cyberbezpieczeństwo głosowania przez internet

Co jakiś czas w debacie publicznej wraca temat wprowadzenia w Polsce możliwości głosowania w wyborach przez internet. Również ostatnio temat odżył w naszym kraju. Pojawiły się m.in. zapowiedzi, że tematyka ta ma być podniesiona na sejmowej podkomisji ds. prawa wyborczego.

Według przedstawiciela tego gremium procedura mogłaby wyglądać następująco: "Po zalogowaniu do aplikacji, przy użyciu profilu zaufanego, pobieralibyśmy kartę do głosowania. Po głosowaniu musiałoby dojść do rozdzielania głosu z podpisem, żeby wybory były tajne. Po zagłosowaniu karta się szyfruje, a nasz podpis jest oddzielany. Karta trafia do elektronicznej urny już bez podpisu, a urna byłaby odkodowywana w dniu wyborów".

Politycy różnych ugrupowań optujących za wprowadzeniem możliwości głosowania przez internet podnoszą m.in., iż skoro bankowość elektroniczna uchodzi za bezpieczną i Polacy ufają aplikacjom bankowym, to również można zapewnić bezpieczeństwo głosowania w ten sposób.

Portal CyberDefence24.pl cytuje też stanowisko Ministerstwa Cyfryzacji w sprawie wprowadzenia głosowania przez internet: „Nie sprowadza się ono wyłącznie do przygotowania zmiany w ustawie, która będzie pozwalała na taką formę głosowania, ale polega przede wszystkim na opracowaniu takich rozwiązań technicznych, które zapewnią wyborcom możliwość należytego uwierzytelnienia się oraz bezpiecznego i tajnego oddania głosu” – wskazuje ministerstwo. Jego zdaniem, mówimy o złożonym zagadnieniu a to „wymusza podjęcie rozważnych działań”.

Warto też przyjrzeć się trochę dokładniej kwestii bezpieczeństwa tego procesu. **Obecny stan wiedzy, jak wskazuje wielu badaczy cyberbezpieczeństwa, pokazuje, że nie jest możliwe w pełni zapewnienie bezpieczeństwa i tajności procesu wyborczego realizowanego przez internet**, a przecież pewność wyników wyborów jest fundamentem demokracji. Zresztą tak samo aplikacje bankowe, ani żadne inne, nie są w pełni bezpieczne. Wszystko jest kwestią zasobów, jakie przeznaczy atakujący. A wrogie nam państwa są w stanie poświęcić nieograniczone środki, aby osiągnąć ten cel, co pokazują m.in. ingerencje w zachodnie procesy wyborcze ze strony Rosji polegające na operacjach informacyjnych i psychologicznych, sianiu dezinformacji i oddziaływaniu na polaryzację społeczną.

Pomimo przykładania ogromnej wagi do zapewnienia wysokiego poziomu cyberbezpieczeństwa w Polsce, w tym także cyfrowych usług publicznych oraz systemów i rejestrów państwowych, nie można dać gwarancji, że głosowanie przy udziale internetu byłoby bezpieczne i anonimowe, a wynik wyborów nie byłby zmanipulowany. Już obecnie, przy braku głosowania przez internet, polskie służby, z wiodącą rolą Agencji Bezpieczeństwa Wewnętrznego i przy znacznym wsparciu NASK, dokonują tytanicznego wysiłku, aby zapewnić cyberbezpieczeństwo wyborów odbywających się w ubiegłym i w tym roku.

Podkreślić należy, że zarówno głosowanie elektroniczne (e-voting), jak i poprzez internet (i-voting) wiążą się z istotnymi ryzykami związanymi z zagrożeniami cyberbezpieczeństwa, których zaistnienie może prowadzić do zmanipulowania wyników wyborów, naruszenia ich tajności oraz równości. Do tego rodzaju ryzyk można zaliczyć np. możliwość upublicznienia na

kogo dana osoba oddała głos, podszywanie się pod inną osobę przy głosowaniu, możliwość cyberataku na system do zliczania głosów. Możliwość ingerencji w procesy wyborcze oparte o przetwarzanie danych w internecie i przy wykorzystaniu urządzeń elektronicznych może zaistnieć w szczególności ze strony służb państw-adwersarzy, grup cyberprzestępczych sponsorowanych przez państwa, czy haktywistów. Inną kwestią jest możliwość zmniejszenia zaufania wyborców do wyników wyborów przeprowadzonych bez fizycznych kart do głosowania i protokołów z komisji wyborczych, co mogłoby prowadzić do podważania wyników wyborów.

Komentarz Niebezpiecznika. Źródło: x.com/@niebezpiecznik

Jak wskazywał dr Łukasz Olejnik, „pod względem technologicznym głosowanie elektroniczne jest jednym z najtrudniejszych do rozwiązania wyzwań [...]. Głosowanie musi być w 100 proc. niezawodne i bezpieczne, a jednocześnie zapewniać brak możliwości oddania kilku głosów przez jedną osobę, tajność, integralność, by raz oddany głos nie mógł zostać zmodyfikowany". Na podobne aspekty zwraca uwagę dr Paweł Zając z Akademii Sztuki Wojennej, który podnosił, iż i-voting nie zapewnia realnej gwarancji zachowania tajności procesu głosowania, a przez to pojawia się pytanie, czy komfort obywateli wynikający z możliwości oddania głosu przez internet nie stoi w sprzeczności z podstawowymi zasadami prawa. W swoim artykule na ten temat zamieścił on cytat z „Diuny" Herberta: „Technologia ma uwodzicielską naturę. Zakładamy, że postępy w tej dziedzinie prowadzą zawsze do korzystnych dla ludzi udogodnień. Oszukujemy sami siebie".

Źródła: WP.pl, CyberDefence24.pl, Niebezpiecznik.pl, Forsal.pl, Cybersecurity and Law.

Atak hakerski na Polską Agencję Prasową (PAP)

W piątek 31 maja 2024 o godzinach 14:00 i 14:20 na stronie internetowej PAP zostały upublicznione fałszywe depesze informacyjne. Mówiły one o ogłoszeniu częściowej mobilizacji wojskowej na terenie Polski. Na podstawie dostępnych informacji, można stwierdzić, że przedstawione zdarzenie musiało być skrupulatnie zaplanowaną operacją hakerską, odznaczającą się dużym zaangażowaniem zasobów: know-how i czasowych. Atak był kombinacją wielu czynników świadczących o wysokim zaawansowaniu organizacyjnym adwersarzy. Wstępne ustalenia i analiza przebiegu działań świadczy, iż podmiot odpowiedzialny za incydent cechował się nie tylko wysokim poziomem kompetencji technicznych zespołu atakującego, ale posiadał również szeroką wiedzę na temat działania polskiego rynku medialnego.


remier RP Donald Tusk: 1 lipca 2024 r.
acznie się w Polsce częściowa mobilizacja

lipca 2024 roku ogłaszona zostanie w Polsce częściowa mobilizacja ojskowa. 200 tysięcy obywateli Polski, zarówno byłych wojskowych, jak i ykłych cywilów zostanie powołanych do obowiązkowej służby wojskowej. szyscy zmobilizowani zostaną wysłani na Ukrainę.

Tytuł i lead depeszy PAP. Źródło: pap.pl

Na podstawie analizy kontekstowej zdarzenia, *modus operandi* adwersarzy oraz potencjalnych szkodliwych dla RP efektów operacji, z grupy podejrzanych za spowodowanie incydentu można wykluczyć ugrupowania haktywistycznych i gangi motywowane finansowo, czy podmioty kierowane ideologicznie.

Wstępna analiza ataku dokonana na podstawie ocen zastosowanej metodologii i dokonanego przez atakujących rozpoznania polskiej sfery medialnej, wskazuje posiadanie świadomości adwersarzy dotyczącej znaczenia depesz PAP dla krajowego rynku informacyjnego.

Do zakładanego celu operacji zaliczyć należy dezinformację dużej skali, zmierzającej do eskalacji poziomu polaryzacji społecznej, wzrostu nastrojów antyukraińskich, a w potencjalnym, radykalnym scenariuszu spowodowania wybuchu niepokojów społecznych i w efekcie masowych antywojennych ruchów o negatywnym wpływie na stabilność wewnętrzną państwa, co w okresie przedwyborczym mogło mieć realny wpływ na wynik wyborów do parlamentu UE.

Zgodnie z tak przyjętymi warunkami, należy zakładać przypisanie odpowiedzialności za dokonanie incydentu – grupom APT kierowanym przez służby specjalne państw wrogo nastawionych Polsce.

Na chwilę obecną za analizę powłamaniową tj. badanie incydentu i atrybutów ataku odpowiadają specjaliści z zespołów bezpieczeństwa teleinformatycznego i informatyki śledczej (*forensic*) ABW przy wsparciu pracowników NASK.

Ze wstępnie udostępnionych publicznie informacji wynika, że wektorem ataku była infiltracja, a następnie infekcja i przejęcie kontroli nad kontem jednego z pracowników PAP, co pozwoliło na przeprowadzenie opisywanego incydentu. Aby uzyskać niezbędne dostępy, atakujący wykorzystali złośliwe oprogramowanie z rodziny tzw. *stealer'ów*. Aplikacje tego rodzaju tworzone są z zamiarem uzyskania nieautoryzowanego dostępu do stacji użytkownika. W efekcie, narzędzia tego typu mają możliwość pozyskiwania z zainfekowanego urządzenia danych i informacji przetwarzanych przez użytkownika danego konta, a następnie przekazanie ich atakującemu. Ten rodzaj złośliwego oprogramowania zwykle jest rozpowszechniany

w ramach kampanii *phishingowych* opartych na socjotechnice, co wykorzystuje najsłabszy z elementów bezpieczeństwa teleinformatycznego, czyli nieuwagę ludzką, a zarazem świadczy o znaczeniu świadomości zagrożeń i konieczności dbania o cyfrową higienę użytkowników.

Wstępna ocena skali szkód związanych z atakiem, pozwala stwierdzić, iż szybka reakcja Ministerstwa Cyfryzacji (MC) i Agencji Bezpieczeństwa Wewnętrznego w obszarze technicznym oraz krajowych mediów na płaszczyźnie komunikacji publicznej umożliwiły ograniczenie potencjalnego, szkodliwego wpływu incydentu bezpieczeństwa na sferę społeczną i informacyjną oraz zniwelowanie zakładanych celów ataku.

W następnie zdarzenia MC potwierdziło kontynuację swojej otwartej polityki informacyjnej wraz działaniami z zakresu podnoszenia świadomości użytkowników Internetu nt. zagrożeń w cyberprzestrzeni. Celem zobrazowania skali ataków polskiej sfery cyfrowej MC rozpoczęło publikację dziennych komunikatów dotyczących zagrożeń w cyberprzestrzeni.

Ponadto potwierdziła się zasadność, a nawet konieczność realizowania prospołecznych kampanii edukacyjnych uświadamiających obywateli RP, że bezpieczeństwo cyberprzestrzeni Polski zależy od każdego z nas, i każdy z nas może stać się nie tylko ofiarą, ale również może zostać wykorzystany przez przestępców jako wektor ataku.

Wykaz depesz PAP. Źródło: pap.pl

Zakłada się, że atak nastąpił prawdopodobnie w wyniku zaniedbań ludzkich. Dlatego każdego zachęcamy do korzystania z materiałów informacyjnych i edukacyjnych dotyczących cyberhigieny oraz szkoleń dla podmiotów KSC przygotowywanych przy współudziale Ministerstwa Cyfryzacji.

Jednakże należy zakładać, że może to być jeden z elementów szerokiej, hybrydowej kampanii wobec Polski stosowanej przez wrogie nam państwa. Warto zachować czujność I reagować na tego rodzaju wydarzenia, aby chronić naszą infrastrukturę i informacje. W sytuacji, gdy zauważyłeś lub podejrzewasz zaistnienie incydentu bezpieczeństwa zgłoś to na stronie właściwego CSIRTu lub na stronie *zgłoś incydent CERT.pl* .

Rekomendacje:

Celem ataków z użyciem tzw. *stealer'ów jest pozyskanie danych logowania do skrzynek mailowych użytkowników biznesowych lub służbowych. Dostęp do wskazanych danych następuje przy pomocy dobrze przygotowanych ataków socjotechnicznych. Obecnie najskuteczniejszą, szeroko dostępną metodą zabezpieczania skrzynek e-mailowych jest stosowanie rozwiązań typ 2FA z wykorzystaniem fizycznego klucza szyfrowania (np. Yubikey), aplikacji autoryzacyjnych, wiadomości SMS/push oraz menagerów haseł. Ponadto w przypadku otrzymania wiadomości spoza organizacji, o treści wskazujących na potrzebę przekazania danych wrażliwych, logowania, pobrania plików, załączników lub oprogramowania zalecamy potwierdzenie procedury alternatywnym kanałem kontaktowym.*

Wzrost zagrożeń deepfake – coraz lepsze rozwiązania wykorzystujące AI do generowania treści

Bez wątpienia mamy do czynienia z bardzo dynamicznym postępem technologicznym w zakresie udoskonalania rozwiązań wykorzystujących AI w tym, celem generowania obrazów oraz plików video. Produkty tzw. 'deepfake' są elementem nowego modelu szerzenia i wykorzystywania fałszywych treści oraz dezinformacji, w sposób o wiele bardziej przekonujący niż dotychczasowo stosowane. Problem polega na tym, że technologia 'deepfake detection' jest nowa i nie rozwija się tak szybko, jak oferowane na rynku rozwiązania do tworzenia treści. Jednym z wyzwań jest m.in. wykorzystywanie automatycznych detektorów niepożądanych treści w Internecie przez np. organy ścigania. Modele oparte na machine learning'u i trenowane na prawdziwych danych mogą mieć kłopot z odsiewaniem prawdziwych treści od tych fałszywie wykreowanych i powielanych z pomocą AI, nie mówiąc już o kwestiach autorstwa danego zdjęcia.

Znany w internecie mem. Źródło: x.com (Twitter)

'LumaAI' ożywiła dobrze znany mem z „imprezy informatyków":

https://x.com/niebezpiecznik/status/1801489242343772223

Dla przykładu sprawdzono również, co się stanie, jeśli spróbujemy „ożywić" następujące statyczne zdjęcia.


Źródło: wikipedia.pl, warszawa.wyborcza.pl

Otrzymano dynamiczne ujęcia powyższych obrazów w formie video mp4 z obrotem kamery i dodaną nową treścią wygenerowaną przez AI. W pierwszym przypadku dodano za pomocą dodatkowej komendy oklaskującą publiczność oraz mówcę na scenie, a w drugim przypadku ruch uliczny. Do tego wystarczyło jedynie darmowe konto na stronie LumaAI.

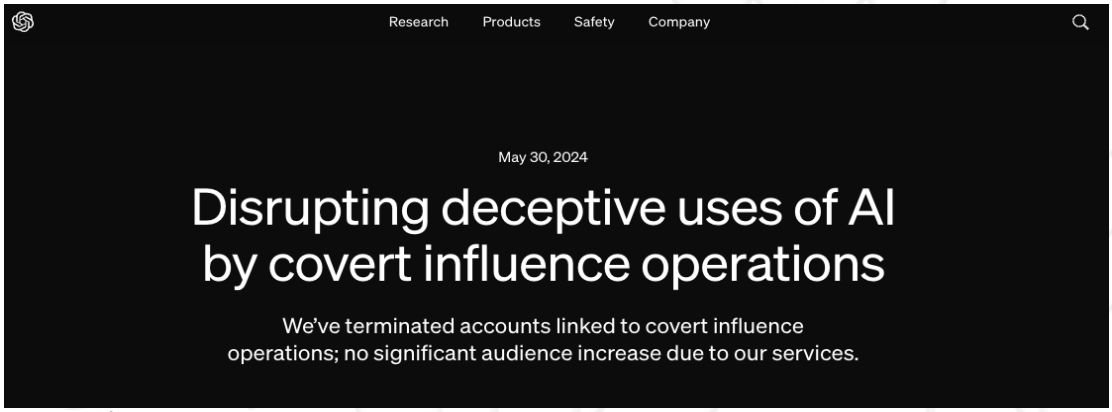
Źródło: lumalabs.ai

Mimo mankamentów w postaci miejscowego rozmycia na ekranie, efekt końcowy jest całkiem zadowalający biorąc pod uwagę minimalny nakład pracy i łatwość generowania. Udowadnia to jak łatwo jest stworzyć materiał video w oparciu o AI i zdjęcie, pokazuje też w jakim kierunku podąża rozwój technologii i jakie zagrożenia może ze sobą nieść, zwłaszcza w odniesieniu do wykorzystania wizerunku danej osoby i manipulacji z tym związanych.

Źródło: openai.com, recordedfuture.com

OpenAI walczy z tajnymi operacjami wywierania wpływu

OpenAI opublikowała swój pierwszy raport dotyczący zagrożeń, w którym podkreślono przypadki, w których firma zlikwidowała konta powiązane z tajnymi operacjami wywierania wpływu. W ostatnim czasie OpenAI stwierdziło, że zakłóciło pięć tajnych operacji wywierania wpływu przy użyciu modeli OpenAI "w celu wspierania zwodniczej działalności w Internecie". W raporcie stwierdzono, że od maja 2024 r. kampanie nie wydają się znacząco zwiększać zaangażowania odbiorców ani zasięgu w wyniku usług związanych z OpenAI.



Źródło: openai.com

Wg. OpenAI podmioty odpowiedzialne za operacje wywierania wpływu wykorzystywały modele sztucznej inteligencji do szeregu zadań, takich jak generowanie krótkich komentarzy i dłuższych artykułów w różnych językach, wymyślanie nazw i biografii dla kont w mediach społecznościowych, prowadzenie badań, debugowanie prostego kodu czy też tłumaczenie i korekta tekstów.

Pełna treść raportu OpenAI dostępna jest na stronie OpenAI pod tym adresem:
https://downloads.ctfassets.net/kftzwdyauwt9/5IMxzTmUclSOAcWUXbkVrK/3cfab518e6b10789ab8843bcca18b633/Threat_Intel_Report.pdf

W raporcie wskazane jest pięć operacji zakłóconych przez OpenAI:

- Wcześniej nieujawniona operacja pochodząca z Rosji, którą OpenAI nazwała "Bad Grammar". Bad Grammar podobno działał głównie na Telegramie i był skierowany do odbiorców na Ukrainie, w Mołdawii, krajach bałtyckich i Stanach Zjednoczonych.
- Wcześniej powiązana z Rosją operacja wpływu "Doppelganger". Według OpenAI, agenci operacyjni Doppelganger (przypisywani przez wiele źródeł jako rosyjskie firmy Structura National Technologies i Social Design Agency) wykorzystywali modele sztucznej inteligencji do tworzenia komentarzy w języku angielskim, francuskim, niemieckim, włoskim i polskim, które były publikowane na X (dawniej Twitter) i 9GAG.
- Wcześniej powiązana z Chinami operacja wpływu "Spamouflage" (aka Empire Dragon).
- Operacja wpływu pochodząca z Iranu i powiązana z Międzynarodową Unią Mediów Wirtualnych (IUVM).
- Operacja wywierania wpływu z siedzibą w Izraelu, powiązana z izraelską firmą STOIC zarządzającą kampaniami politycznymi, którą OpenAI określa jako "Zero Zeno".

Warsztaty w ramach priorytetu empact

W dniach 27-29 maja 2024 r. Centralne Biuro Zwalczania Cyberprzestępczości zorganizowało warsztaty w ramach priorytetu EMPACT Cyberataki OA 6.3. W warsztatach poza policjantami CBZC, udział wzięli przedstawiciele organów ścigania z Hiszpanii, Rumunii i Macedonii Północnej.

Celem warsztatów było wypracowanie dobrych praktyk w państwach członkowskich poprzez omówienie zrealizowanych spraw oraz wymianę doświadczeń i wiedzy specjalistycznej w zakresie zwalczania cyberprzestępczości i pojawiających się nowych sposobów działania sprawców. Omawiane sprawy koncentrowały się w szczególności na tematyce cyberprzestępczości jako usługa (CaaS) i spieniężania środków pochodzących z tych przestępstw poprzez wykorzystanie kryptowalut. Jednym z elementów warsztatów było podzielenie się sposobami i innowacyjnymi metodami radzenia sobie z obecnymi i pojawiającymi się zagrożeniami cyberprzestępczością.

W szkoleniu udział wzięli funkcjonariusze CBZC oraz przedstawiciele zagranicznych organów ścigania z Północnej Macedonii, Hiszpanii i Rumunii, którzy zaprezentowali przykłady zrealizowanych spraw. Obecni na warsztatach funkcjonariusze przedstawili struktury i zadania jednostek zajmujących się zwalczaniem cyberprzestępczości funkcjonujących w tych państwach i wypracowali kanały bezpośredniej wymiany informacji.

Zrealizowane warsztaty z całą pewnością wniosą nowe rozwiązania w sposoby zwalczania przestępczości internetowej i zapobiegania cyberzagrożeniom. Spotkanie wzmocni również, funkcjonującą na bardzo dobrym poziomie, współpracę międzynarodową.

Więcej informacji: *https://cbzc.policja.gov.pl/bzc/aktualnosci/347,Warsztaty-w-ramach-priorytetu-EMPACT.html*

Warsztaty zorganizowane przez CBZC. Źródło: cbzc.policja.gov

Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta

W maju 2024 roku CSIRT KNF wykrył i zgłosił do zablokowania 5 646 domen (w kwietniu 6 345 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.).

Podobnie jak pisaliśmy w minionych miesiącach, również w maju 2024 trwał scenariusz znany pod nazwą „fraud inwestycyjny". To metoda, w której przestępcy podszywają się pod znane osoby lub instytucje, celem nakłonienia potencjalnej ofiary do zainwestowania środków i otrzymania wysokiej stopy zwrotu. Równie niezmiennie cyberprzestępcy wykorzystują scenariusz znany jako „scam na kupującego" w trakcie, którego ofiarami padają osoby wystawiające produkty i/lub usługę na sprzedaż. W związku ze zbliżającym się okresem wakacyjnym przestępcy zmienili motyw wykorzystywany w fałszywych sklepach. Obecnie najczęściej spotkać możemy się z zachęta do zakupienia basenów lub mebli i sprzętu ogrodowego w wyjątkowo niskiej cenie. W rzeczywistości przestępcy mają na celu wyłudzenie przelewu na zarządzany przez siebie rachunek. Jak co miesiąc, celem pozyskania danych uwierzytelniających do bankowości elektronicznej oraz danych kart płatniczych, atakujący podszywali się pod polskie banki. Strony phishingowe dystrybuowali poprzez wiadomości e-mail oraz fałszywe reklamy w mediach społecznościowych. Przestępcy podszywając się pod Bank Pekao opublikowali reklamę na platformie Facebook. Pod pretekstem rzekomej możliwości otrzymania zwrotu za zakupy, zachęcali do kliknięcia w link, który prowadził na złośliwą stronę. Na niej ofiara zachęcana była do instalacji fałszywej aplikacji. Analiza wykazała, że złośliwa aplikacja była przygotowana w technologii PWA/WebAPK. Otwarcie aplikacji powodowało próbę załadowania w trybie pełnoekranowym adresu strony phishingowej. Kampania ta miała prawdopodobnie na celu wyłudzanie danych uwierzytelniających do bankowości elektronicznych.

Kampania, której nie obserwowaliśmy wcześniej było podszycie pod rzekomo zwolnionego pracownika sieci KFC. W nagraniu video, które w rzeczywistości zostało przygotowane w technologii deepfake, informował on, że poda tajne kody zniżkowe od zakupu jedzenia. Z materiałem zapoznać się można pod adresem: *https://x.com/CSIRT_KNF/status/1792488904014086552*. W rzeczywistości atakujący podstawili fałszywą stronę pośrednika płatności oraz imitacje stron bankowości elektronicznej wybranych polskich banków. Analizowaliśmy również kampanie phishingowa podszywającą się pod firmę BLIK. Informowali o rzekomej możliwości odebrania nagrody. Do dystrybucji stron phishingowych wykorzystali reklamy na platformie Facebook. W rzeczywistości wyłudzali kody BLIK. W kolejnej analizowanej przez nas kampanii phishingowej cyberprzestępcy informowali o rzekomej możliwości wykupienia zagubionej paczki lub porzuconego bagażu za 9 zł. W rzeczowości była to strona phishingowa mająca na celu wyłudzenie danych kart płatniczych. Następnie przestępcy starali się wyprowadzać środki z rachunków, wykorzystując do tego „model subskrypcyjny". Z kolei atakujący podszywając się pod Pocztę Polską oraz InPost, informowali o rzekomej konieczności aktualizacji adresu dostarczenia przesyłki. W rzeczywistości wyłudzali dane kart płatniczych. Podobne kampanie phishingowe miały już kilkukrotnie miejsce w latach 2023 i 2024. Przestępcy przygotowali

również kampanię phishingową, w której podszywając się pod członka rodziny, rozsyłali wiadomości SMS, prosząc o kontakt poprzez WhatsApp, wykorzystując link, który podawali w wiadomości SMS. Następnie prowadzili konwersację tekstową, podczas której przekonywali do zrobienia przelewu na podany przez nich numer rachunku. Były to konta bankowe zarządzane przez przestępców.

Jedną z metod ochrony przed wymienionymi wyżej i innymi działaniami cyberprzestępców jest wiedza. Dlatego (jak zawsze) zachęcamy do śledzenia informacji o bieżących schematach i scenariuszach przestępczych na naszych profilach w mediach społecznościowych: X (Twitter), LinkedIn oraz Facebook.

Dodatkowo informujemy, iż w związku z tym, że ataki ransomware stanowią aktualnie jedno z najpoważniejszych zagrożeń dla bezpieczeństwa organizacji, to wspólnie z polskimi ekspertami cyberbezpieczeństwa opracowaliśmy dokument, w którym opisujemy możliwe sposoby zabezpieczenia organizacji oraz przedstawiamy propozycje reagowania w przypadku wystąpienia incydentu ransomware. Dokument przygotowany został w dwóch wersjach językowych.

Link do opracowania tutaj:

- język polski: https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/Aktualnosci?articleId=89341&p_id=18
- język angielski: https://www.knf.gov.pl/en/?articleId=89410&p_id=19

Źródło: CSIRT KNF

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.