Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

10/2024

SPIS TREŚCI

AntyDDoS-owa tarcza Ministerstwa Cyfryzacji

Cyberatak typu DDoS (ang. Distributed Denial of Service) jest to atak na system komputerowy lub usługę w celu uniemożliwienia działania poprzez zajęcie wszystkich dostępnych zasobów lub pasma. Ataki te wykonywane są najczęściej przez zainfekowane komputery, nad którymi przejęto kontrolę przy użyciu szkodliwego oprogramowania. Obecnie ataki DDoS można kupić jako usługę w darknecie. Dokonują ich zarówno grupy APT powiązane z wrogimi państwami (np. aby zablokować ważne dla danego kraju strony internetowe i świadczone przez nie usługi), jak również haktywiści, aby dokonać demonstracji swoich możliwości w ważnych dla nich sprawach.

W obliczu pogarszającej się sytuacji bezpieczeństwa na świecie, cyberataki, w tym DDoS, są coraz większym problemem w państwach NATO i UE. Mogą one sparaliżować ważne procesy zarówno dla bezpieczeństwa państwa, działalności gospodarczej, jak równię usług kluczowych dla obywateli. Przykładowo, w Polsce wśród incydentów poważnych zgłoszonych w 2023 r. w sektorze bankowości i infrastruktury rynków finansowych znalazły się 4 incydenty poważne związane z atakami DDoS. W ich wyniku dochodziło do częściowej lub całkowitej niedostępności usług bankowości elektronicznej.

W związku z upowszechnieniem się ataków DDoS na serwisy ważne dla funkcjonowania i bezpieczeństwa państwa, **Ministerstwo Cyfryzacji sfinansowało i zleciło NASK-PIB realizację projektu AntyDDoS**: „Zapewnienie usługi ochrony przed atakami DDoS – Distributed Denial of Service dla podmiotów realizujących zadania publiczne oraz podmiotów istotnych z punktu widzenia bezpieczeństwa RP". Dzięki tym działaniom na chwilę obecną osłonę przed atakami DDoS **Ministerstwo Cyfryzacji zapewnia centralnie dla 76 instytucji, w tym administracji państwowej, jak również dla Sił Zbrojnych RP oraz służb specjalnych**. Warto więc podkreślić, że Ministerstwo Cyfryzacji roztacza tarczę antyDDoS-ową nie tylko nad podmiotami cywilnymi, ale także nad Wojskiem Polskim.

Logo projektu AntyDDoS

Ataki typu DDoS stanowią także zagrożenie dla firm prywatnych działających w Polsce. Mogą one korzystać z dostępnych na rynku rozwiązań dających ochronę przeciwko tego typu cyberatakami. Aby budować polską suwerenność technologiczną państwo polskie zleciło w ramach Narodowego Centrum Badań i Rozwoju prace badawczo-rozwojowe dotyczące rozwiązań przeciwko atakom DDoS. Ich wyniki zostały już wdrożone i są dostępne na rynku pod nazwą TAMA. Dzięki temu polskie firmy mogą korzystać z w pełni polskiego rozwiązania z zakresu cyberbezpieczeństwa. TAMA jest wciąż rozwijana w ramach NCBR.

Aby zwiększyć poziom odporności danej organizacji na ataki DDoS warto też zapoznać się z dobrymi praktykami przygotowanymi przez CISRT KNF.

Źródło: Ministerstwo Cyfryzacji, Exatel, CSIRT KNF.

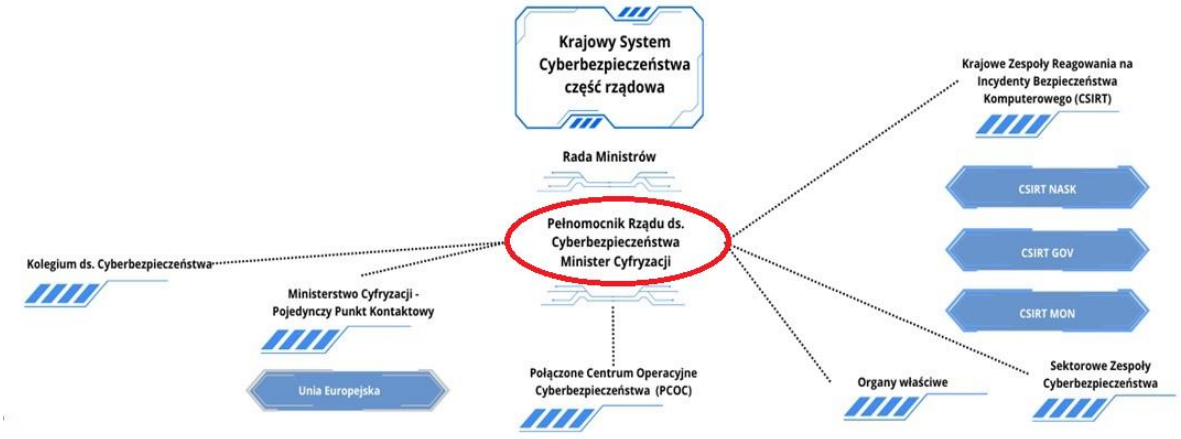
Instrumenty w rękach Pełnomocnika Rządu ds. Cyberbezpieczeństwa

Wraz z wejście w życie w 2018 r. ustawy o krajowym systemie cyberbezpieczeństwa ustanowiona został funkcja Pełnomocnika Rządu ds. Cyberbezpieczeństwa. Dotychczas funkcję tę pełniły osoby z kierownictwa resortu cyfryzacji, a obecnie Wicepremier i Minister Cyfryzacji. Przygotowywana nowelizacja ustawy przewiduje na stałe przypisanie tej funkcji do Ministerstwa Cyfryzacji.

Do zadań Pełnomocnika należy koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa, co przekłada się m.in. na uprawnienia związane z analizą funkcjonowania Krajowego Systemu Cyberbezpieczeństwa, upowszechnianie nowych rozwiązań cyberbezpieczeństwa, inicjowanie krajowych cyberćwiczeń, współpraca międzynarodowa, wspieranie badań naukowych i rozwój technologii, jak również podnoszenie świadomości społeczeństwa w zakresie cyberbezpieczeństwa.

Ustawa daje także w ręce Pełnomocnika konkretne narzędzia, które wymiernie przekładają się na odporność polskiej cyberprzestrzeni. Procedowana nowelizacja ustawy o KSC przewiduje wzmocnienie roli Pełnomocnika.

W obecnym stanie prawnym Pełnomocnik może przede wszystkim wydawać rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania. W bieżącym roku wydano już trzy, jedna dotyczyła aktualizacji produktów Fortinet, druga Biuletynów Informacji Publicznej, a trzecia oprogramowania Zimbra Collaboration. Ich wdrożenie przez podmioty KSC pozwala uniknąć wystąpienia incydentu krytycznego. Ponadto, Pełnomocnik wydaje swoje komunikaty. W tym roku wydał cztery, które dotyczyły: ataków DDoS, zabezpieczenia infrastruktury teleinformatycznej administracji samorządowej na terenach zagrożonych powodzią, podszywania się pod ważnych polityków oraz wzrostu liczby incydentów związanych z wyciekiem danych.



Pozycja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w Krajowym Systemie Cyberbezpieczeństwa

Z kolei przygotowywana zmiana ustawy o KSC da Pełnomocnikowi nowe instrumentarium pozwalające szerzej oddziaływać na cyberbezpieczeństwo naszego kraju. Po pierwsze, wzmocniony zostanie mechanizm rekomendacji.

Po drugie, planowane jest wprowadzenie mechanizmu pozwalającego wykluczać zidentyfikowane produkty lub usługi od dostawców wysokiego ryzyka, których

wykorzystywanie stanowiłoby zagrożenie dla bezpieczeństwa państwa. W tym miejscu należy podkreślić, że proces ten będzie w pełni transparentny i oparty o konkretne kryteria techniczne. Procedura obejmować będzie zarówno poziom merytoryczno-techniczny (z udziałem CSIRT-ów), jak i zatwierdzenia przez najważniejsze organy państwa w ramach Kolegium ds. Cyberbezpieczeństwa, w tym z udziałem Pełnomocnika.

Po trzecie, wprowadzona zostanie instytucja polecenia zabezpieczającego. Polecenie to będzie mogło być wydane przez Ministra Cyfryzacji (a przypomnijmy, że funkcja ta będzie powiązana z Pełnomocnikiem) w przypadku wystąpienia incydentu krytycznego, w celu skoordynowania efektywnej reakcji na ten incydent. Przed wydaniem polecenia zabezpieczającego niezbędne będzie przeprowadzenie analizy uzasadniającej wydanie tych środków nadzwyczajnych. Będzie ona przeprowadzana wspólnie z Zespołem do spraw incydentów krytycznych, w którego skład wchodzą CISRT-y poziomu krajowego, RCB oraz Pełnomocnik i Minister Cyfryzacji. Następnie Minister Cyfryzacji będzie mógł wydać w drodze decyzji administracyjnej polecenie zabezpieczające odnoszące się do incydentu krytycznego. Będzie w nim zawarte wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się. Wprowadzenie do polskiego porządku prawnego polecenia zabezpieczającego (z rygorem natychmiastowej wykonalności) jest konieczne dla zapewnienia bezpieczeństwa narodowego w obliczu coraz częstszych i poważniejszych cyberataków.

Po czwarte, projektowane przepisy dają też możliwość Pełnomocnikowi zlecenia udzielenia wsparcia przez CSIRT poziomu krajowego innemu podmiotowi KSC. To uprawnienie pozwoli Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa skutecznie reagować na zagrożenia i szybko zapewnić niezbędne wsparcie podmiotom dotkniętym incydentami.

Po piąte, projekt ustawy zakłada, że prowadzenie wspomnianego Zespołu ds. Incydentów Krytycznych przejmie od Dyrektora RCB Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa. Dotychczasowa praktyka prac Zespołu pokazała, że takie rozwiązanie będzie bardziej efektywne.

Po szóste, przy Pełnomocniku sformalizowane zostanie funkcjonowanie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), kluczowego dla koordynacji działań państwa w obszarze cyberbezpieczeństwa i skutecznego reagowania na incydenty.

Po siódme, Pełnomocnik będzie również mógł zlecać przeprowadzanie badań i ekspertyz oraz tworzyć zespoły robocze. Te kompetencje zapewnią mu dodatkowe narzędzia do realizacji jego zadań.

Po ósme, inne organy państwa będą miały obowiązek udzielania wsparcia Pełnomocnikowi, tak aby w sytuacji gdy dane zagadnienie dotyczy ich właściwości otrzymał on niezbędną pomoc.

Opisany powyżej katalog przyszłych uprawnień Pełnomocnika Rządu ds. Cyberbezpieczeństwa istotnie wzmocni jego rolę w zapewnianiu cyberbezpieczeństwa na poziomie całego kraju, a także wymiernie zwiększy efektywność i sprawność funkcjonowania Krajowego Systemy Cyberbezpieczeństwa.

Źródło: Ministerstwo Cyfryzacji

Technologia Passkey: przyszłość bezpiecznego logowania?

Stale rosnący poziom zagrożeń w sferze cyfrowej oraz zwiększające się zaawansowanie techniczne atakujących sprawia, że tradycyjne formy zabezpieczenia kont wyłącznie hasłami przestały być wystarczająco efektywne. Powyższe, potwierdzają obserwowane w ostatnich latach dynamiczne zmiany rynkowych standardów związanych z implementacją nowych polityk haseł, menagerów haseł czy technologii uwierzytelniania wieloskładnikowego (*2FA/MFA*), jak np.: via SMS, tokeny aplikacji czy klucze fizyczne.

FidoAlliance.org

W odpowiedzi na nadchodzące wyzwania bezpieczeństwa, fundacja non-profit *Fast Identity Online Alliance (FIDO Alliance)* zrobiła krok wyprzedzający i upubliczniła nowy, otwarty standard uwierzytelniania o nazwie *Passkey*.

Jak działa *Passkey*? Jest to rodzaj rozwiązania kryptograficznego, który zastępuje tradycyjne hasła. Wykorzystuje on pary kluczy publicznych i prywatnych do uwierzytelniania użytkowników generowanych przez użytkownika podczas tworzenia nowego konta lub logowania do usługi. Klucz publiczny jest przechowywany na serwerze dostawcy usługi, natomiast klucz prywatny pozostaje na urządzeniu użytkownika (podobnie do *PGP*), takim jak smartfon czy komputer. Podczas logowania, użytkownik jest proszony o autoryzację za pomocą biometrii (np. odcisku palca lub obrys twarzy) lub kodu PIN, wtedy urządzenie podpisuje żądanie za pomocą klucza prywatnego i przesyła je do serwera, który weryfikuje podpis za pomocą klucza publicznego. Zgodnie z powyższym, nawet jeśli klucz publiczny zostanie przechwycony, nie zostanie on użyty do uzyskania dostępu do konta bez klucza prywatnego.

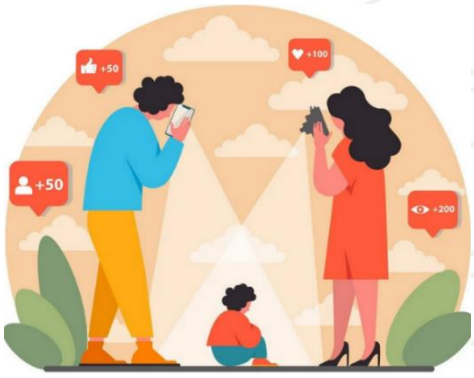
Technologia *Passkey*, oparta na standardzie *FIDO*, zyskuje na popularności jako nowoczesne rozwiązanie uwierzytelniania użytkowników. Obiecuje nie tylko wyższy poziom bezpieczeństwa, ale także większą wygodę użytkowania. Na wzrost popularności rozwiązania wpływa, umożliwienie wykorzystania go przez największe światowe firmy technologiczne, jak m.in. *Google*, *Apple* i *Microsoft*, które są członkami *FIDO Alliance* oraz wspierają rozwój i wdrażanie technologii *Passkey*. Dzięki czemu technologia ta, staje się kompatybilna i możliwa do wykorzystania na wielu różnych platformach i urządzeniach. Jednakże powyższe wciąż stanowi jedne z głównych wyzwań stojących przed technologią – konieczność szerokiej adaptacji przez deweloperów istniejących systemów uwierzytelniania oraz edukacji użytkowników na temat nowych metod logowania.

Podsumowując, technologia *Passkey* ma potencjał, aby zrewolucjonizować sposób w jaki uwierzytelniamy się w sieci. Jest to krok w stronę przyszłości bez haseł. Choć rozwiązanie wymaga szerokiej adaptacji i implementacji, to potencjał w zakresie poprawy bezpieczeństwa i wygody jest ogromny. Wraz z rozwojem technologii, możemy spodziewać się rosnącej liczby podmiotów ją wspierających, co przyczyni się do bezpieczniejszego i bardziej wygodnego korzystania z Internetu.

Źródło: FIDOAlliance.org, google.com/account/about/passkeys/,

Sharenting i bezpieczeństwo dziecka w sieci

Sharenting to termin opisujący aktywność rodziców, szczególnie w mediach społecznościowych, polegającą na częstym zamieszczaniu zdjęć oraz treści dotyczących ich dzieci. Pojęcie to powstało z połączenia dwóch angielskich słów: *share* (dzielić się, rozpowszechniać) oraz *parenting* (rodzicielstwo). Choć sharenting jest stosunkowo nowym zjawiskiem, można wyróżnić kilka jego odmian: ***Oversharenting*** — nadmierne dzielenie się materiałami dotyczącymi dziecka w mediach społecznościowych, np. zakładanie mu konta na Facebooku, Instagramie lub *YouTube*. ***Parental trolling*** — przedstawianie wizerunku dziecka w sposób prześmiewczy lub kompromitujący. ***Commercial sharenting*** — upublicznianie wizerunku dziecka dla zysku, co może prowadzić do kreowania „młodych influencerów". ***Prenatal sharenting*** — publikowanie obrazów z badań prenatalnych. ***Family sharenting*** — udostępnianie zdjęć dzieci w internecie przez innych członków rodziny, nie tylko rodziców.



www.scmp.com

Sharenting stał się powszechnym zachowaniem współczesnych rodziców; dokumentowanie życia dziecka w Internecie bywa uznawane za normę społeczną. *Raport London School of Economics* z 2018 roku wykazał, że aż 75% rodziców aktywnych w Internecie regularnie udostępnia zdjęcia lub filmy swoich dzieci, szczególnie gdy dzieci są młodsze. W Polsce około 40% rodziców publikuje zdjęcia dzieci, a 25% robi to średnio raz w tygodniu. Jednym z głównych problemów związanych z *sharentingiem* jest ryzyko naruszenia prywatności dziecka. Upublicznianie zdjęć i szczegółowych informacji może prowadzić do stworzenia „cyfrowego śladu" dziecka, co w przyszłości może być źródłem wstydu lub problemów w kontaktach z rówieśnikami. Materiały w sieci pozostają tam często na stałe, co może powodować długotrwałe negatywne skutki.

Sharenting może również narażać dziecko na zagrożenia fizyczne. Udostępnianie lokalizacji lub szczegółowych informacji na temat miejsca pobytu dziecka może ułatwić identyfikację przez osoby niepożądane. W dobie nowoczesnych technik, takich jak *deepfake*, upublicznianie wizerunku dziecka wiąże się z dodatkowymi zagrożeniami — można łatwo wygenerować zmanipulowane materiały z twarzą dziecka, co może posłużyć do szantażu, hejtu, czy niewłaściwego wykorzystania.

Jak się przed tym chronić? Czy należy całkowicie zrezygnować z publikowania zdjęć dzieci? Dobrą praktyką jest publikowanie materiałów w taki sposób, aby dziecko było niewidoczne lub nie do rozpoznania, np. fotografując je od tyłu lub zamazując twarz. Warto przed publikacją rozważyć, czy zdjęcie nie ujawnia zbyt wielu danych, takich jak adres czy szczegóły związane ze szkołą. Warto również unikać zdjęć wrażliwych, np. przedstawiających dziecko w bieliźnie lub stroju kąpielowym. Pamiętajmy w sieci nic nie ginie i raz wrzucone w Internet zdjęcie zostanie tam na zawsze.

Źródło:. Ejournals.eu, pewniwsieci.pl, apcz.umk.pl

AI jako cel cyberataków

Sztuczna inteligencja (AI) rozwija się w zawrotnym tempie, stając się jednym z kluczowych elementów współczesnych systemów technologicznych. Jej zastosowanie obejmuje coraz więcej obszarów: od medycyny i finansów, aż po autonomiczne pojazdy i systemy obronne. Jednak równocześnie, jak pokazują raporty i badania, AI staje się również nowym celem dla cyberprzestępców. Ataki na systemy oparte na sztucznej inteligencji, takie jak modele uczenia maszynowego, niosą ze sobą poważne konsekwencje, w tym utratę danych, zmanipulowane decyzje systemów i naruszenie prywatności.

exai.pl

AI, a zwłaszcza systemy uczenia maszynowego, mają specyficzne podatności, które są chętnie wykorzystywane przez cyberprzestępców. Wg OWASP (*Open Web Application Security Project*) ataki na ai można podzielić na:

Atak na dane wejściowe (*Input Manipulation Attack*) polega on na wprowadzeniu przez atakującego zmodyfikowanych danych wejściowych w celu oszukania modelu uczenia maszynowego. Takie manipulacje mogą prowadzić do błędnych wyników, mimo że zmiany są często niezauważalne dla człowieka. Obrona przed tymi atakami obejmuje trenowanie modeli odpornych na takie zmiany, walidację danych wejściowych oraz monitorowanie anomalii. Atak może obejmować m.in. manipulację obrazami lub manipulacja ruchem sieciowym w celu uniknęcia wykrywania włamań.

Atak zatrucia danych (*Data Poisoning Attack*) polega na manipulacji danymi treningowymi, co prowadzi do błędnego działania modelu uczenia maszynowego. Aby się przed nim chronić, ważne jest stosowanie walidacji danych, bezpiecznego przechowywania oraz kontroli dostępu do danych. Ponadto, monitorowanie anomalii, audyty, oraz walidacja modeli są kluczowe. Przykładem ataku może być celowe wprowadzenie błędnych danych do klasyfikatora spamu, co zmienia sposób, w jaki model klasyfikuje maile.

Atak typu model *Inversion*. Ten rodzaj ataku polega na odwróceniu działania modelu przez atakującego, aby wydobyć z niego poufne informacje. Przykładem może być kradzież danych osobowych z modelu rozpoznawania twarzy poprzez analizę jego odpowiedzi.

Atak inferencji członkostwa (*Membership Inference Attack*) polega na manipulowaniu danymi treningowymi, aby ujawnili, czy konkretne dane zostały użyte w procesie uczenia modelu. Aby się przed tym chronić, stosuje się techniki takie jak losowe mieszanie danych, obfuskację modelu oraz monitorowanie. Przykładem ataku jest próba uzyskania poufnych danych finansowych, poprzez sprawdzenie, czy określony rekord był częścią zbioru danych treningowych.

Atak kradzieży modelu (*Model Theft*) polega na zdobyciu przez atakującego dostępu do parametrów modelu, co pozwala na jego skopiowanie i wykorzystanie. Aby się przed tym bronić, należy stosować szyfrowanie, kontrolę dostępu, regularne kopie zapasowe, obfuskację kodu oraz znaki wodne. Przykład ataku to kradzież modelu przez konkurenta w celu uzyskania przewagi rynkowej.

Ataki na łańcuch dostaw w uczeniu maszynowym (*ML Supply Chain Attacks*) polega na atakowaniu łańcucha dostaw oprogramowania uczenia maszynowego, takich jak platformy *MLOps*, oprogramowanie do zarządzania danymi, modele i inne. Aby się przed nimi chronić, należy weryfikować integralność pakietów, stosować bezpieczne źródła, aktualizować oprogramowanie oraz zapewniać silną kontrolę dostępu. Ataki te mogą doprowadzić do kompromitacji infrastruktury i wycieku danych.

Ataki na transfer uczenia (*Transfer Learning Attack*) polegają na wykorzystaniu modelu, który został wytrenowany na jednym zadaniu, a następnie dostosowany do innego, co powoduje jego niepożądane działanie. Zapobieganie obejmuje monitorowanie i aktualizowanie zbiorów danych, używanie zaufanych danych, izolowanie modeli, stosowanie prywatności różnicowej i przeprowadzanie audytów bezpieczeństwa. Atak może prowadzić do błędnych wyników, naruszeń poufności, szkód reputacyjnych oraz problemów prawnych

Ataki przekształcenia modelu (*Model Skewing*) polegają na manipulowaniu rozkładem danych treningowych, aby model działał w sposób niepożądany. Zapobieganie obejmuje stosowanie silnych kontroli dostępu, weryfikację autentyczności danych, techniki walidacji i czyszczenia danych, detekcję anomalii oraz regularne monitorowanie wyników modelu. Takie ataki mogą prowadzić do błędnych decyzji, strat finansowych, uszczerbku na reputacji oraz szkód, zwłaszcza w krytycznych aplikacjach używanych np. do diagnozowania w medycynie.

Ataki na integralność wyników (*Output Integrity Attack*) polegają na manipulowaniu wynikami modelu uczenia maszynowego, aby wpłynąć na jego zachowanie lub zaszkodzić systemowi. Zapobieganie obejmuje stosowanie metod kryptograficznych, bezpiecznych kanałów komunikacyjnych, walidację wyników, prowadzenie niezatrzaskujących się logów, regularne aktualizacje oprogramowania oraz audytowanie wyników. Takie ataki mogą prowadzić do utraty zaufania do wyników, strat finansowych lub zagrożeń w krytycznych aplikacjach, takich jak diagnostyka medyczna.

Ataki na zatrucie modelu (*Model Poisoning*) polegają na manipulacji parametrami modelu, aby wpłynąć na jego wyniki w sposób niepożądany. Zapobieganie obejmuje stosowanie technik rekuraryzacji, projektowanie odpornych modeli oraz technik kryptograficznych do ochrony parametrów modelu. Takie ataki mogą prowadzić do błędnych wyników, np. w systemach bankowych, gdzie model identyfikuje numery na czekach, prowadząc do finansowych strat.

openai.com

Rozwój AI stawia przed nami ogromne możliwości, ale i wyzwania związane z bezpieczeństwem. Coraz większe zastosowanie tej technologii w kluczowych sektorach, takich jak finanse, zdrowie czy bezpieczeństwo, czyni ochronę tych systemów priorytetem. W przyszłości cyberprzestępcy będą stosować bardziej zaawansowane techniki do ataków na AI, by manipulować wynikami lub zdobywać dane. Organizacje musza inwestować w skuteczne badania i wprowadzanie nowych standardów bezpieczeństwa, a do tego potrzebna jest współpraca miedzy ekspertami AI i ekspertami Cyberbezpieczeństwa.

Źródła: owasp.org, atlas.mitre.org, drmalinowski.edu.pl, nask.pl

Krzywdzili dzieci – zostali zatrzymani przez policjantów CBZC!

Mężczyzna podszywał się pod agencję reklamową, wyłudzając w ten sposób zdjęcia o charakterze seksualnym małoletnich dzieci. W innym przypadku to kobieta wykorzystywała seksualnie swojego małoletniego syna, następie udostępniała i sprzedawała zarejestrowane z tych czynów materiały. To tylko dwa przykłady z wielu ujawnionych przestępstw...

Działania na terenie całego kraju – ponad milion plików zabezpieczonych

Przeszło 400 funkcjonariuszy Centralnego Biura Zwalczania Cyberprzestępczości z całego kraju wzięło udział w dwutygodniowej operacji „ENOLA GAY", w wyniku której zatrzymano 75 osób w wieku od 16 do 78 lat. Wśród podejrzanych o posiadanie, rozpowszechnianie i produkowanie materiałów przedstawiających seksualne wykorzystywanie małoletnich osób, było 10 kobiet. Przeprowadzono 112 przeszukań, w wyniku których zabezpieczono ponad 7,5 tysiąca różnego rodzaju sprzętu cyfrowego, zawierającego ponad milion plików przedstawiających seksualne wykorzystywanie małoletnich (telefony, komputery, laptopy, dyski, pendrive itp.). Ujawniono rekordowe ilości zdjęć i filmów – u jednego z podejrzanych zabezpieczono 430 tysięcy zdjęć z treściami pedofilskimi, u innego ok. 150 tysięcy nagrań.

Materiał operacyjny CBZC

Materiał operacyjny CBZC

Krzywda dzieci:

- Jeden z mężczyzn skradł i wykorzystywał wizerunek jednej z agencji reklamowych, co umożliwiło późniejsze wyłudzanie od kobiet zdjęć o charakterze seksualnym ich małoletnich dzieci.
- Kobieta podżegana przez 6 mężczyzn, wykorzystywała seksualnie swojego małoletniego syna, a następie udostępniała i sprzedawała osobom poznanym na portalu randkowym zarejestrowane z tych czynów materiały.
- Mężczyzna rozpowszechniał pliki wideo zawierające treści z seksualnym wykorzystaniem małoletnich osób.

To tylko przykłady przestępczej działalności w sieci. Walka z przestępcami dotyczącymi wykorzystywania dzieci w Internecie jest jednym z priorytetowych zadań policjantów.

Zarzuty karne:
Podejrzani usłyszeli zarzuty karne posiadania, rozpowszechniania i produkowania treści o charakterze pedofilskim. Jeden z podejrzanych usłyszał również zarzut kradzieży tożsamości, tj. podszywania się pod firmę. W 31 przypadkach sądy zadecydowały o zastosowaniu środków zapobiegawczych w postaci tymczasowych aresztów. Maksymalna kara za publiczne prezentowanie treści pornograficznych wynosi nawet do 15 lat pozbawienia wolności.

Materiał operacyjny CBZC

Policjanci CBZC kolejny raz uderzyli w sprawców przestępstw o charakterze seksualnym
Efekty działań to wynik pracy analitycznej i operacyjnej policjantów CBZC. Cała akcja była ściśle koordynowana z Departamentem ds. Cyberprzestępczości i Informatyzacji Prokuratury Krajowej oraz z prokuratorami terenowymi z całego kraju. Realizowane działania wspierane były również przez funkcjonariuszy komend powiatowych i miejskich Policji.

Wspólny cel to zwalczanie przestępczości internetowej o podłożu seksualnym!

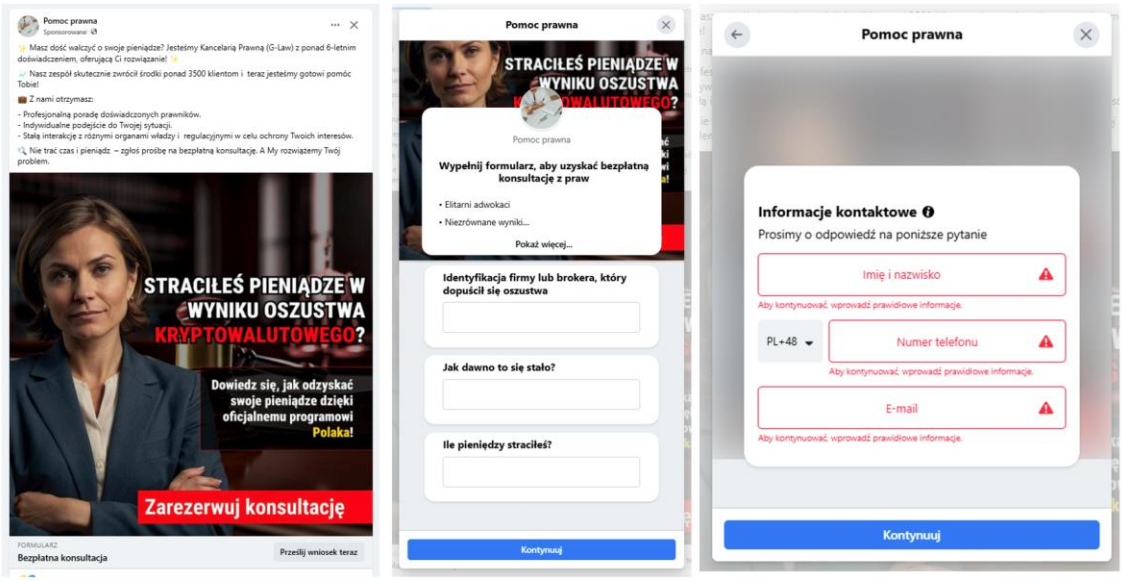
Więcej na temat: ***https://cbzc.policja.gov.pl/bzc/aktualnosci/433,Krzywdzili-dzieci-zostali-zatrzymani-przez-policjantow-CBZC.html***

Podsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta

W październiku 2024 roku *CSIRT KNF* wykrył i zgłosił do zablokowania 4 324 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 7 396 domen. A na koniec omawianego miesiąca, na liście hole znajdowało się 245 638 domen.

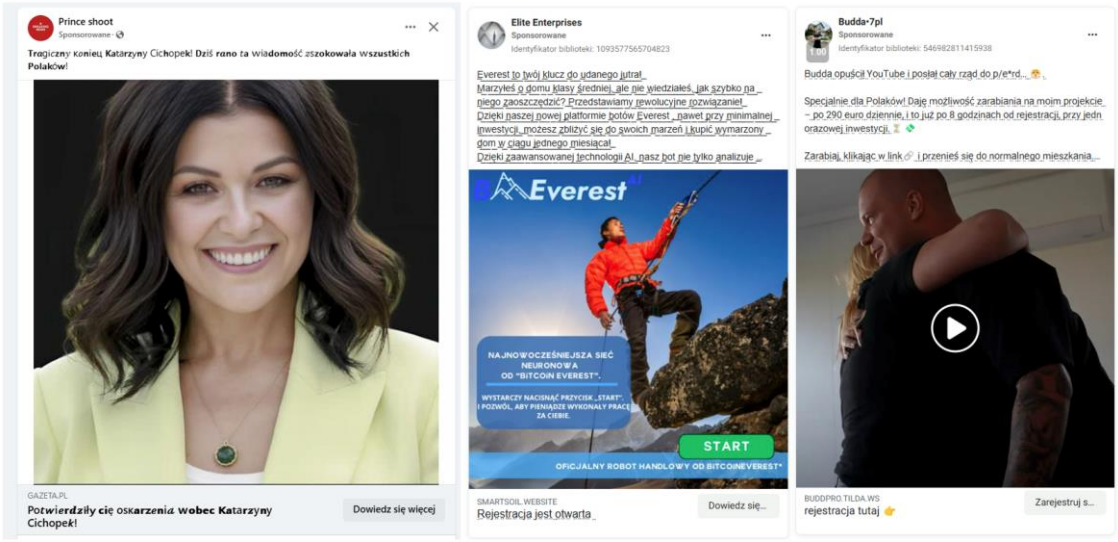
W związku ze znaczącą liczbą fałszywych reklam publikowanych na platformie Facebook promujących rzekomą możliwość inwestowania, a w rzeczywistości powodujące wysokie straty finansowe u klientów banków, *CSIRT KNF* wypracował mechanizmy wykrywające takie działanie przestępcze oraz procesy przekazywania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

W minionym miesiącu ciekawym zjawiskiem jest fakt, że największy procent wykrytych reklam dotyczył rzekomej możliwości „odzyskania środków". To drugi etap omawianego schematu działania przestępców, w którym 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.

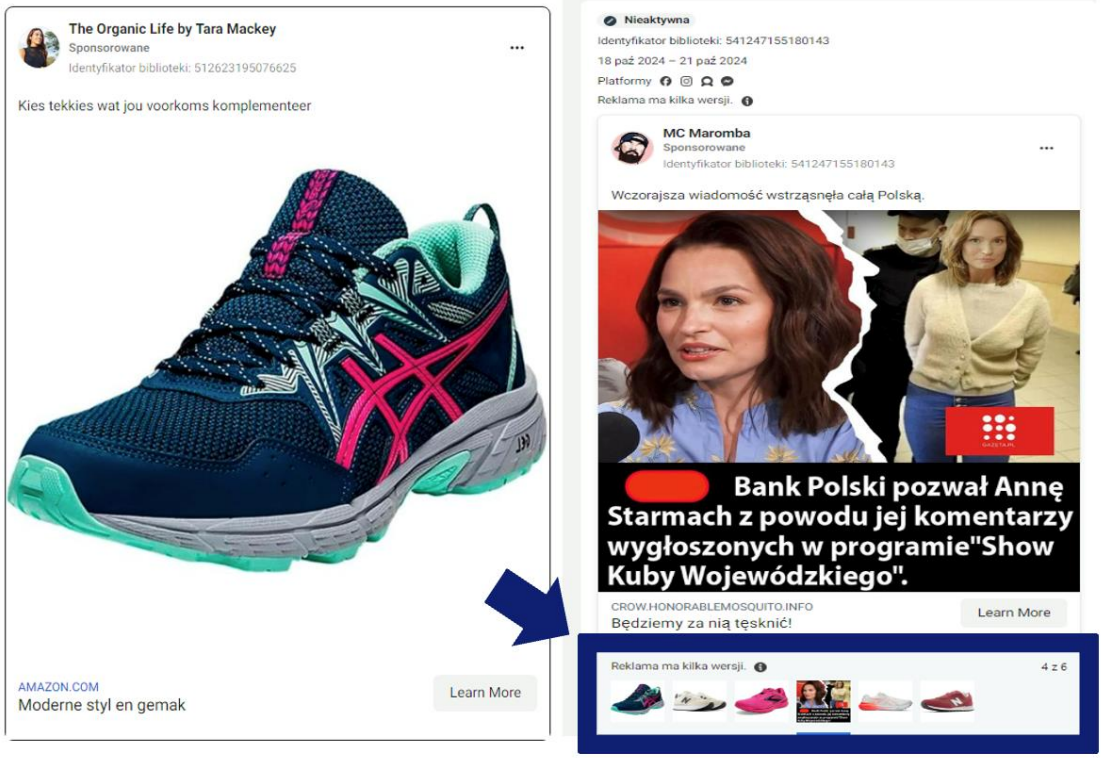


Atakujący zdają sobie również sprawę z tego, że publikowane reklamy są przez nich wykrywane, dlatego podejmują serię kroków mających na celu maskowanie dystrybuowanej przez nich treści. Przykładowymi działaniami są:

- manipulacja sposobem zapisu treści reklamy:



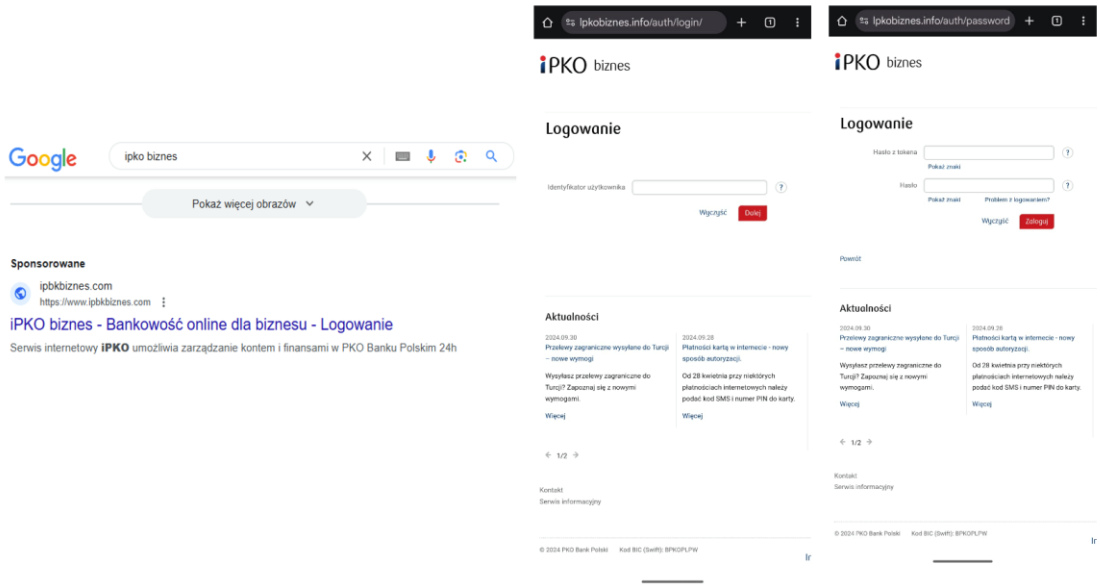
- wersjonowanie reklamy:



- wydłużanie nagrań deepfake:

Z przykładami stworzonych przez przestępców nagraniami video, przy wykorzystaniu deepfake, można zapoznać się pod adresem: *https://cebrf.knf.gov.pl/deepfake*

Zidentyfikowaliśmy również kampanie przestępcze podszywające się bezpośrednio pod podmioty z sektora finansowego. Przestępcy wykorzystują wizerunek banków wyłudzają m.in informacje o kartach płatniczych, dane uwierzytelniające do bankowości elektronicznej, czy kody *BLIK*. Przestępcy publikowali reklamy na platformie *Facebook*, wysyłali wiadomości SMS oraz wykorzystywali pozycjonowanie w wyszukiwarce *Google*. W kampaniach przestępczych informowali m.in. 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.



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*.

Statystki zgłoszeń i incydentów CSIRTów poziomu krajowego:

Zestawianie danych z CSIRTów poziomu krajowego:						
	Jednostkowo miesięcznie:		Średnia tygodniowa:		Średnia dzienna:	
	Zgłoszenia	Incydenty	Zgłoszenia	Incydenty	Zgłoszenia	Incydenty
za miesiąc sierpień:						
NASK	35417	7393	8854,3	1848,3	1142,5	238,5
C:[SIRT/MON]	2883	320	720,8	80,0	93,0	10,3
Zbiorcze:	***38300***	***7713***	***9575,0***	***1928,3***	***1235,5***	***248,8***
za miesiąc wrzesień:						
NASK	40819	6999	10204,8	1749,8	1360,6	233,3
C:[SIRT/MON]	2738	383	684,5	95,8	91,3	12,8
Zbiorcze:	**43557**	**7382**	**10889,3**	**1845,5**	**1451,9**	**246,1**
za miesiąc październik:						
NASK	36779	7491	9194,8	1872,8	1186,4	241,6
C:[SIRT/MON]	2626	384	656,5	96	84,7	12,4
Zbiorcze:	**39405**	**7875**	**9851,3**	**1968,8**	**1271,1**	**254,0**
Zestawienie za kwartał:						
NASK	**113015**	**21883,0**	**9417,9**	**1823,6**	**1241,9**	**240,5**
C:[SIRT/MON]	**8247**	**1087,0**	**687,3**	**90,6**	**90,6**	**11,9**
Zbiorcze:	**121262**	**22970,0**	**10105,2**	**1914,2**	**1332,5**	**252,4**

Zestawienie danych statystycznych otrzymanych od CSIRTów poziomu krajowego.

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.