Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

12/2023

SPIS TREŚCI

Sprawa kursów walutowych w Google, czyli… nie mamy pana płaszcza!

W poniedziałek 1 stycznia br. Internet obiegła wieść o spadku kursu Złotego o ponad 20% wobec euro i dolara, jak wskazywała wyszukiwarka *Google*. Minister finansów uspokajał na X (dawniej *Twitter*), że to „fejk" (błąd źródła danych). Ministerstwo Finansów oraz Ministerstwo Cyfryzacji zażądały wyjaśnień od koncernu *Google*. Firma uważa jednak, że jest jedynie wyszukiwarką, więc nie ingeruje w dane, jakie są prezentowane; nie weryfikuje ich i nie gwarantuje również, że są dokładne, powołując się na wyłączenie swojej odpowiedzialności.

„Fejkowe" załamanie złotego w danych pokazywanych przez Google. Zrzut ekranu. *Źródło: HomoDigital*

Odpowiedź koncernu zbulwersowała dziennikarzy i ekspertów. Małgorzata Fraser z portalu *CyberDefence24* ironizowała, że *Google* po prostu nie interesuje się szkodą wywołaną na peryferyjnym dla siebie rynku, a Big Techy traktują Polskę jak cyfrową kolonię. Krzysztof Izdebski, prawnik i aktywista zajmujący kwestiami transparentności i technologii stwierdził, że *„Google albo nie radzi sobie w PR, albo wypiera ze świadomości wpływ, który ma… w zasadzie na wszystko. Jeśli nie jest w stanie weryfikować informacji, które wyróżnia i które mogą spowodować powszechne zakłócenia to… niech ich nie publikuje w ten sposób"*. W sposób sarkastyczny odniósł się do sytuacji również współzałożyciel think-tanku *Global.Lab* Adam Traczyk, pisząc, iż *„Google ogólnie nic nie może. To tylko najczęściej odwiedzana strona internetowa świata, której firma matka wyceniana jest na 1,75 biliona dolarów"*.

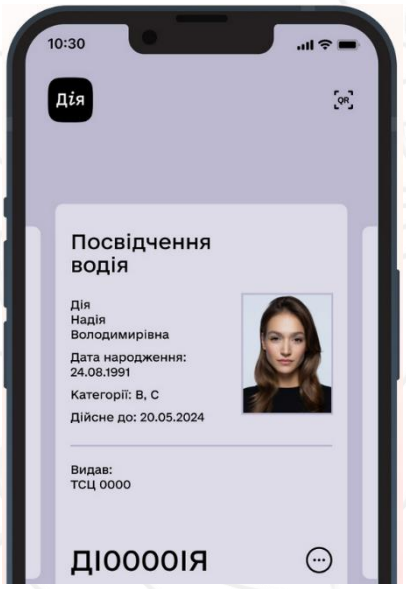
Sprawa jednak jest poważna i dotyczy też odpowiedzialności innych platform internetowych, jak np. *Facebook*, *Uber*, *Booking*, *Airbnb*. Odniósł się do niej wicepremier, minister cyfryzacji Krzysztof Gawkowski. Stwierdził, że nie jest usatysfakcjonowany odpowiedzą Google, uważa, że zabrakło staranności oraz zapowiedział uregulowanie tej kwestii, aby określić odpowiedzialność platform za publikowane dane. W tym wypadku nie miało to wielkiego wpływu na rynek, ale w przyszłości mogą wystąpić sytuacje znacząco oddziałowujące na gospodarkę oraz bezpieczeństwo państwa i społeczeństwa. Obecnie nie ma rozwiązań prawnych zmuszających platformy do weryfikacji danych, jednak wkrótce powstaną. Polska będzie wdrażać *Digital Service Act*. Celem unijnego rozporządzenia jest zwiększenie bezpieczeństwa użytkowników, transparentność działań platform internetowych, budowanie solidnych narzędzi moderowania treści i bardziej odpowiedzialnych reklam oraz ochrony danych osobowych, a także skutecznych mechanizmów skarg i odwołań.

Jako użytkownicy Internetu sami też musimy pamiętać o weryfikacji informacji w sieci, np. weryfikując też inne źródła, aby nie dać się oszukać.

Źródła: X, RMF FM, CyberDefence24, Gazeta.pl, strona Ministerstwa Cyfryzacji.

Aplikacja Diia – cyfrowe usługi publiczne w warunkach wojennych

Jeszcze przed pełnoskalową agresją Rosji na Ukrainę w lutym 2022 r. nasz wschodni sąsiad realizował ambitne reformy cyfryzacji kraju wprowadzając wiele cyfrowych usług publicznych. Wielką popularność zyskiwała aplikacja *Diia*, która umożliwia załatwianie spraw urzędowych, odpowiednik polskiego *mObywatela*. Cyfryzacja usług publicznych, wraz z przeniesieniem danych rządowych (i nie tylko) do chmury, umożliwiała zapewnienie ciągłości funkcjonowania państwa w warunkach wojennych.



Źródło: diia.gov.ua

Jednak rewolucyjne zmiany w sferze ukraińskiej cyfryzacji zaszły już po rosyjskiej inwazji, gdy konieczne stało się szybkie poszerzenie katalogu usług online. Z *Dii* korzysta obecnie prawie 20 mln Ukraińców (*mObywatel* ma ok. 15 mln użytkowników).

Na portalu internetowym oraz w aplikacji mobilnej dostępnych jest ponad 130 usług, z czego ponad 30 zostało uruchomionych w 2023 r., a od wybuchu wojny wprowadzono ponad 70 nowych funkcjonalności – od kompleksowej obsługi osób wewnętrznie przesiedlonych po program *eRobota*. Wśród nich są m.in. usługi budowlane, wniosek o zawarcie małżeństwa online, przerejestrowanie samochodu. W *Diia* uruchomiono też program *eOdbudowa*. Tysiące Ukraińców, których domy zostały uszkodzone w wyniku rosyjskiej agresji, mogło otrzymać pomoc finansową na remont. *Ukraińskie Ministerstwo Transformacji Cyfrowej* (MTC) planuje też uruchomienie *Diia.Office*, oddzielnej usługi dla korpusu Służby Cywilnej.

Wkrótce po wybuchu pełnoskalowej wojny, dzięki współpracy polskiego i ukraińskiego resortu cyfryzacji, w polskim *mObywatelu* dodano aplikację *Diia.pl*, która umożliwia Ukraińcom przebywający w Polsce posługiwanie się elektronicznym dokumentem tożsamości oraz załatwianie online szeregu spraw.

Diia posiada też integracje z chatbotami o zastosowaniu obronnym, np. opracowany przez MTC *eVorog*, który pozwala cywilom dostarczać wojsku informacje o ruchach rosyjskich wojsk. *eVorog* jest też zintegrowany z aplikacją wojskową *Delta*, systemem zarządzania polem walki.

W ostatnim czasie podjęto decyzję o uruchomieniu interaktywnej mapy schronów w aplikacji *Diia*. W aplikacje dostępne będą adres i zdjęcia schronu, dane o jego pojemności i rodzaju. Ponadto będzie można ocenić stan schronu, złożyć skargę lub sugestię. Władze państwowe i samorządowe będą zobowiązane do stałego aktualizowania informacji o schronach, a także monitorować ich stan i dostępność.

W ostatnim czasie w Ukrainie gorącym tematem jest kwestia uchylania się od służby wojskowej, w projekcie ustawy skierowanej do parlamentu pojawiła się m.in. propozycja rozsyłania powołań drogą elektroniczną, choć jeszcze dzień wcześniej wicepremier ds. cyfryzacji Mychajło Fedorow miał zapewniać, że wezwań przez *Diia* nie będzie nigdy.

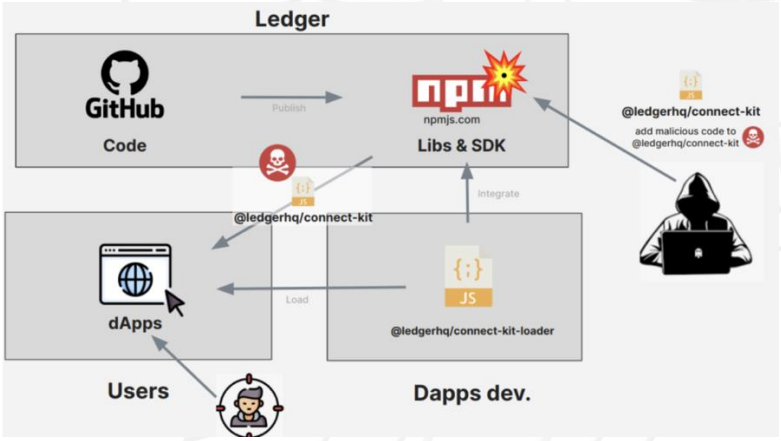
Źródła: thedigital.gov.ua, GazetaPrawna.pl

Kradzież ok. 600.000 USD z portfela kryptowalutowego Ledger

Ledger to jeden z bardziej rozpowszechnionych na świecie sprzętowych portfeli do przechowywania kryptowalut. Firma dostarczająca ww. produktfunkcjonuje na rynku od 2014 r., a jej rozwiązania cieszą się uznaniem użytkowników na całym świecie. Niestety 14 grudnia 2023 r. były pracownik firmy *Ledger* padł ofiarą wyrafinowanego ataku phishingowego.

Atakujący uzyskał dostęp do jego konta *NPMJS* (menadżer pakietów dla *Javascript* współdzielonego między aplikacjami), omijając 2FA przy użyciu tokenu sesji. Atakujący opublikował na *NPMJS* złośliwą wersję *Ledger Connect Kit* (trzy złośliwe wersje modułu 1.1.5, 1.1.6, 1.1.7). W wyniku tego rozprzestrzenione zostało złośliwe oprogramowanie do innych aplikacji zależnych od modułu. *Connect Kit* mianowicie umożliwia podłączenie *DApps* (krótkich zdecentralizowanych aplikacji) do portfeli sprzętowych *Ledgera*. Kod umożliwiał przekierowywanie zasobów do portfeli hakerów. Według producenta, firmy *Ledger*, zespoły technologiczne i bezpieczeństwa zostały powiadomione o ataku, a oryginalna wersja poprawki *Ledger Connect Kit* została wdrożona przez zespoły *Ledger* w ciągu 40 minut od momentu, gdy *Ledger* dowiedział się o ataku. Ze względu na charakter sieci CDN (*Content Delivery Network*) i mechanizmów buforowania w Internecie, złośliwy plik pozostawał dostępny nieco dłużej. Od skompromitowania *NPMJS* do całkowitego rozwiązania minęło około 5 godzin. Ta wydłużona dostępność złośliwego kodu wynikała z czasu potrzebnego CDN na globalną propagację i aktualizację pamięci podręcznej o najnowszą, oryginalną wersję pliku.

Portfel kryptowalut i NFT Ledger



Schemat przebiegu ataku, Źródło: ledger.com

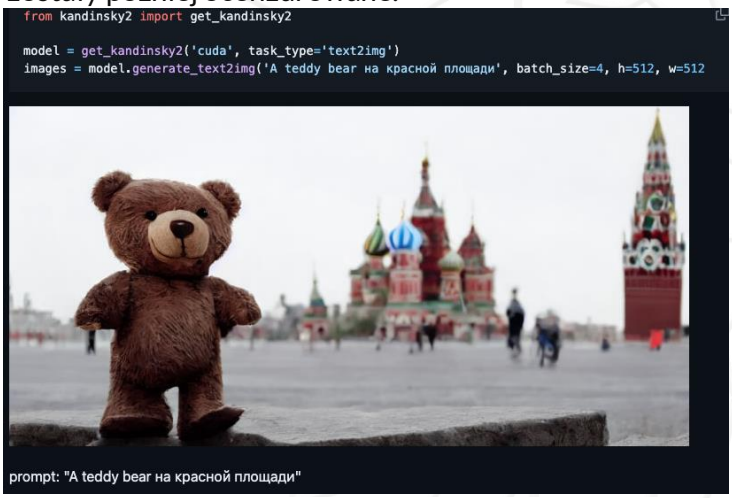
Komentarz: *Łańcuch infekcji rozpoczął się od ataku phishingowego na pracownika, co jest częstym zabiegiem stosowanych przez grupy hakerskie. Warto przestrzegać zasad cyberhigieny i nie klikać w podejrzane linki otrzymywane w wiadomościach SMS oraz e-mail. Zalecana jest ostrożność przy korzystaniu z urządzeń do przechowywania kryptowalut, regularne aktualizacje i monitorowanie komunikatów producentów.*

Źródła: ledger.com, checkmarx.com, kapitanhack.pl, bleepingcomputer.com

Rosja posiada swojego konkurenta ChatGPT: GigaChat od Sberbanku – dążenia w kierunku niezależności

Sztuczna Inteligencja (AI) to szybko rozwijająca się dziedzina, która ma wiele zastosowań i implikacji dla różnych dziedzin i sektorów. *ChatGPT* może generować tekst, kod, historie, dowcipy i nie tylko, wykorzystując przetwarzanie i generowanie języka naturalnego. W kwietniu 2023 r. Rosja przedstawiła swojego konkurenta *ChatGPT*: ***GigaChat***, chatbota od *Sberbank*, rosyjskiego bank, będącego częściowo własnością rosyjskiego rząd, który znacząco inwestuje w technologię, aby zmniejszyć zależność Rosji od Zachodu.

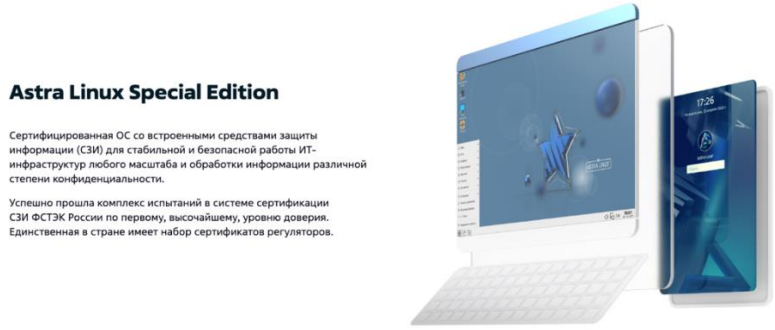
Obecna wersja *GigaChat* nie jest realnym konkurentem do *ChatGPT*. Rozwój projektu jest hamowany m.in. przez wpływ łańcucha dostaw i sankcji na pozyskiwanie procesorów graficznych. Surowe wymagania *Sberbanku* jeśli chodzi o dostęp do aplikacji w tym śledzenie nazwisk, numerów paszportów, adresów IP jest istotną przesłanką o braku zagrożenia pod względem wykorzystania *GigaChat* do tworzenia złośliwych aplikacji choćby dlatego że dostęp jest limitowany. Oprócz *GigaChat*, Rosjanie opracowali również projekt o nazwie „***Kandinsky 2.2***" jako odpowiedź na m.in. *Midjourney* do kreowania obrazów z wykorzystaniem AI. Początkowe wersje *GigaChat* i *Kandinsky* nie były w pełni zgodne z rosyjską retoryką polityczną, dlatego zostały później ocenzurowane.



Obraz wygenerowany przez oprogramowanie 'Kandinsky 2.2, Źródło: github.com/ai-forever/Kandinsky-2

Inne rosyjskie, narodowe projekty to np. alternatywa dla *Windows OS* – ***Astra Linux***, rosyjska dystrybucja *Linux* oparta na systemie operacyjnym *Debian GNU/Linux* której 1800 licencji zakupiła m.in. rosyjska *Duma* (po zawieszeniu licencji *Microsoftu*). W tym miesiącu na stronie *atomic-energy.ru* pojawiła się informacja, iż twórcy oprogramowania *Astra Linux* zamierzają pomóc rosyjskiej kolei oraz spółce *Rosatom* w zastąpieniu *„importowanego oprogramowania"* ich własnym. Na stronie producenta znajdujemy następujące informacje dot. dystrybucji *Astra Linux*: *„Certyfikowany system operacyjny z wbudowanymi systemami ochrony informacji (IPS) do stabilnego i bezpiecznego działania infrastruktury IT dowolnej skali i przetwarzania informacji o różnych poziomach poufności. Pomyślnie przeszedł zestaw testów w systemie certyfikacji systemów ochrony Federalnej Służby Kontroli Technicznej i Eksportowej Federacji Rosyjskiej (FSTEC Rosji) zgodnie z pierwszym, najwyższym poziomem zaufania. Jest to jedyna firma w kraju, która posiada*

zestaw certyfikatów regulacyjnych.” Astra Linux początkowo był opracowany dla krajowych agencji wojskowych i wywiadowczych.



Źródło: astralinux.ru

Globalny wyścig technologiczny trwa – rosyjski rząd w lutym 2020 opracował „***AI Roadmap***” z budżetem 244 bilionów rubli na rozwój AI (*Sberbank* zaoferował 112 bilionów rubli). Jednakże warto mieć na uwadze również malejącą liczbę talentów AI w Rosji, na który ogromny wpływ miała wojna z Ukrainą i ucieczka wielu specjalistów.

Rosja od dawna chciała stworzyć własny Internet, często nazywany ***Runetem***, który działałby niezależnie od reszty świata i był zgodny z rosyjskimi przepisami. Ostatnie dwa lata sprawiły, że jej ambicje stały się bardziej osiągalne, ponieważ wielu zachodnich gigantów technologicznych, w tym *Apple*, *Microsoft* i *Google*, zawiesiło lub ograniczyło swoje usługi w kraju, zachęcając użytkowników i firmy do przejścia na rosyjskie alternatywy. Ale choć przejście na rodzimy sprzęt i oprogramowanie jest przekonujące dla autorytarnych reżimów, takich jak rosyjski, jego wdrożenie napotyka wiele przeszkód, choćby te związane z sankcjami. Zgodnie z prawem jednak, agencje rządowe muszą całkowicie zrezygnować z zagranicznego oprogramowania do 2025 r. Kolejnym przykładem mógł być plan rosyjskiego giganta telekomunikacyjnego *Rostelecom*, który miał dostarczyć urzędnikom telefony z systemem operacyjnym ***Aurora***, które miały stanowić rodzimą alternatywę dla *Iphone’a*. Jednakże projekt nie zyskał popularności.

Komentarz: *Istotnymi kwestiami mającymi wpływ na rynek produktów technologicznych w Rosji jest cena. Ceny rosyjskich produktów wzrosły o ponad 20% od marca 2022 r. Jeśli cena jest za wysoka, a alternatywne rozwiązania technologiczne mniej atrakcyjne, Rosjanie będą poszukiwać dostępu do zachodnich technologii za pośrednictwem sprzedawców w Azji i Turcji. Trudno przewidzieć jak rosyjski rynek technologiczny i internetowy będzie wyglądał za kilka lat, jednakże faktem jest, że Rosjanie próbują znaleźć sposoby „na przejście przez cyfrową kurtynę bez jej zerwania”. Nawet uwzględniając sankcje, Rosja jest częścią globalnej gospodarki w tym cyfrowej i być może nikt (a szczególnie Rosja) nie jest gotowy na całkowite odcięcie od świata.*

Źródła: tristwolff.medium.com, therecord.media, cloudbooklet.com, cyberdefence24.pl

Chińskie platformy deep i darkwebowe – alternatywą dla zachodnich forów

W ostatnich latach nastąpił znaczny wzrost aktywności ze strony Chin w *dark i deep web*. Mimo wyzwań stawianych przez chiński tzw. „***Wielki Firewall***" (kontrolowanie aktywności w Internecie, cenzura, zablokowanie dostępu do wybranych aplikacji i stron internetowych), Chińczycy radzą sobie poprzez korzystanie z VPN (choć o tym też władza w Chinach doskonale wie). Niemniej jednak, warto mieć na uwadze rosnący w ostatnim czasie potencjał chińskich forów hakerskich w *dark i deep web*.

Brak regulacji i nadzoru ze strony zachodnich agencji na chińskim rynku handlu w *dark web*, oferuje „*bezpieczny*" ekosystem do przestępczych działań. Obecnie dwa wiodące i rywalizujące chińskie fora *dark web* to ***Deepmix*** i ***Chang'an*** **(**również występujące pod nazwą Chang'an Sleepless Night**)**. Oba rzekomo stawiają na pierwszym miejscu bezpieczeństwo i anonimowość swoich użytkowników, jednocześnie oskarżając się wzajemnie o oszustwa.

Od czasu ich uruchomienia, fora te zyskały znaczną popularność wśród traderów i kupujących poszukujących bezpiecznej i anonimowej platformy do prowadzenia działalności. *Deepmix* został założony w 2013 r. i możemy tam znaleźć oferty nielegalnych towarów, usług głównie dedykowanych dla chińskich użytkowników. Pomimo ataków *DDoS Deepmix* stanowi jedno z głównych forów w chińskim ekosystemie darknetu. W przypadku *Chang'an*, został on uruchomiony w 2022 r. i szybko stał się jednym z największych w branży. *Chang'an* ma oficjalną grupę *Telegram „@cabyc*", która rozpoczęła działalność w tym samym roku i od tego czasu stała się popularna wśród użytkowników. Grupa stanowi forum dla użytkowników do zadawania pytań, dzielenia się wskazówkami i otrzymywania aktualizacji na temat rynku. *Chang'an* posiada przyjazny dla użytkownika interfejs strony internetowej zawiera wbudowaną funkcję kontaktu z administratorem.

Komentarz*: Istotne jest, iż od czasu zamknięcia niektórych z bardziej znanych, zachodnich forów darknetu np. Genesis Market, pojawiły się znaczące zmiany w chińskim darknecie. Przewiduje się, że osoby nie mówiące po chińsku mogą również zacząć częściej korzystać z chińskich forów, ponieważ zachodnie, anglojęzyczne platformy są lepiej monitorowane przez agencje rządowe i służby. Otwiera to również pole dla cyberprzestępców do swobodnej wymiany usług.*

Główna strona forum Deepmix, Źródło: cyberint.com

Główna strona forum Chang'an, Źródło: webz.io

Źródła: webz.io, cyberint.com, Recorded Future

Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta

W grudniu 2023 roku przestępcy nie pozwolili się nudzić analitykom bezpieczeństwa. Tylko w minionym miesiącu jako CSIRT KNF wykryliśmy i zgłosiliśmy do zablokowania 2 345 domeny, które wcześniej zakwalifikowaliśmy jako wyłudzające dane. Za ich pomocą przestępcy próbowali pozyskać loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe (*imię*, *nazwisko*, *adres zamieszkania*, *e-mail*, *numer telefonu etc.*).

Podobnie jak we wcześniejszych miesiącach, również w grudniu nieustannie trwały kampanie znane pod nazwą „*fraud inwestycyjny*", w których przestępcy podszywają się pod znane osoby lub instytucje, celem nakłonienia potencjalnej ofiary do zainwestowania środków i otrzymania wysokiej stopy zwrotu. W rzeczywistości prowadzą grę psychologiczną, mającą na celu narażanie ofiary na wysokie starty finansowe. Coraz częściej, atakujący wykorzystują technologię *deepfake* do tworzenia fałszywych nagrań.

Deepfake to technologia wykorzystująca sztuczną inteligencję do generowania realistycznych filmów lub dźwięków, które są manipulacjami. *Deepfake* wykorzystują techniki uczenia maszynowego i sztucznych sieci neuronowych do naśladowania wyglądu, głosu i manier osoby, tworząc fałszywe materiały wideo lub audio, które mogą wyglądać i brzmieć jak rzeczywiste.

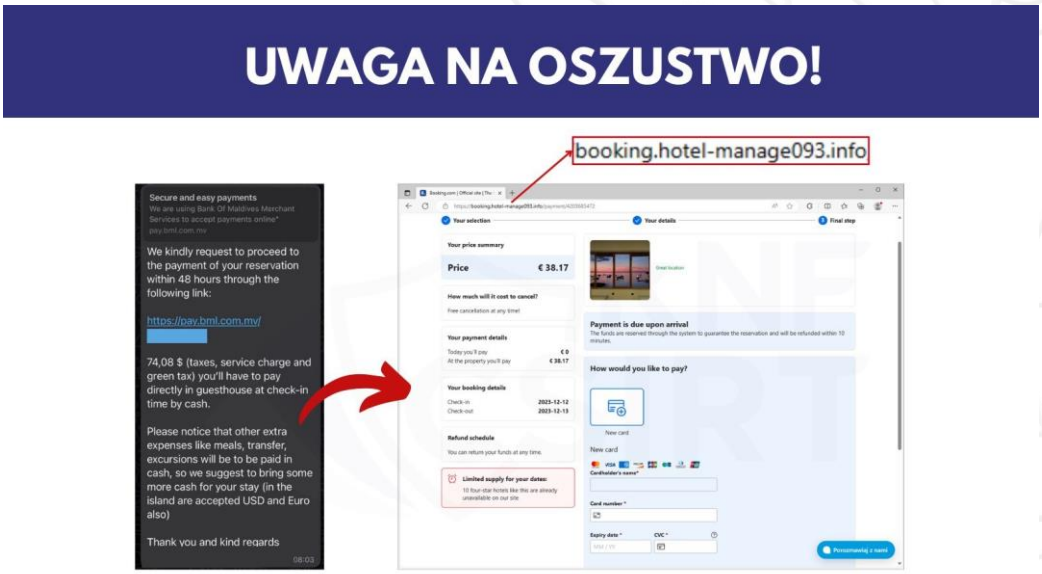
Tym sposobem, ofiary nie tylko widzą statyczne zdjęcie znanej osoby, ale także mogą zobaczyć (często) realistycznie wyglądające nagranie, w którym znajoma twarz, rozpoznawalnym dla niej głosem informuje, że rzekomo zarobiła na inwestycji, którą reklamuje. To sprawia, że materiał przestępczy staje się jeszcze bardziej wiarygodny. Sama technologia *deepfake* rodzi duże zagrożenie, a atakujący wykorzystują ją coraz częściej do swoich działań.

Znanym od lat sposobem dystrybucji domen *phishingowych* są wiadomości SMS. W grudnia 2023 roku atakujący nadal wykorzystywali tę drogę dystrybucji domen *phishingowych*, jednocześnie wykorzystując powtarzające się często scenariusze. W minionym miesiącu podszywali się pod bank *PKO BP*, firmy kurierskie takie jak *InPost* oraz *UPS*, a także *Pocztę Polską*. W każdym z tych przykładów, wiadomość SMS informowała o zdarzeniu, które wymagało pilnego kliknięcia w zawarty w niej link. Były to strony *phishingowe*, na których przestępcy zachęcali do wpisania danych kart płatniczych. Wpisane tam informacje trafiały w ręce przestępców, którzy następnie starali się wykonać operacje fraudowe. Podobnie, jak w poprzednich miesiącach 2023 roku, również w grudniu do dystrybucji domen *phishingowych* przestępcy, oprócz wiadomości SMS, wykorzystywali również reklamy w mediach społecznościowych, czy wiadomości e-mail. Poprzez platformę *Facebook*, publikowali posty zachęcające do zakupów przedmiotów znanych marek, w konkurencyjnych cenach. W rzeczywistości, w reklamach zawarty był link prowadzący do strony *phishingowej*, łudząco przypominającej strony takich sklepów jak *Mohito*, czy *Wojas*. Również tą drogą, zachęcali do rzekomej możliwości zdobycia karty *ZTM* w konkurencyjnej cenie, w rzeczywistości wykradając dane kart płatniczych. Zarówno w listopadzie'23, jak i grudniu'23 przestępcy przeprowadzili kampanie phishingową podszywająca się pod *GOV*. Rozesłali wiadomości e-mail, powołując się za rzekomą możliwość odebrania zwrotu nadpłaconego podatku za rok 2022, zachęcali do kliknięcia w link. W rzeczywistości poszkodowany trafiał na *phishingową* stronę, gdzie

wyłudzane były od niego dane. Nadal trwa również kampania podszywającą się pod *Booking*. Poniżej przedstawiamy schemat działania tego ataku:

1. Właściciele hoteli otrzymują fałszywe zapytania rezerwacyjne w formie wiadomości e-mail ze złośliwym oprogramowaniem.
2. Po zainfekowaniu urządzenia, przestępcy kradną dane logowania do platformy *Booking*.
3. Następnie tworzą fałszywe oferty i strony *phishingowe*, oszukując klientów hoteli.
4. Fałszywe strony są przesyłane do klientów poprzez *Booking* lub inne kanały.

Opublikowaliśmy raport dotyczący tego działania, obejmując temat od strony analizy *Cyber Threat Intelligence*. Zachęcamy do zapoznania się z nim: https://cebrf.knf.gov.pl/images/Booking_-_rezerwacja_malware.pdf



Na koniec tego krótkiego podsumowania, warto zaznaczyć, że w krajobrazie zagrożeń coraz wyraźniej widać piętno wykorzystania sztucznej inteligencji przez cyberprzestępców. Zarówno w zakresie wykorzystania technologii *deepfake*, jak i różnych modeli (językowych, wizyjnych, systemów ekspertowych i innych). Z tego powodu, rozpoczęliśmy cykl publikacji dotyczących sztucznej inteligencji.

Pierwszy artykuł jest już dostępny pod adresem: https://cebrf.knf.gov.pl/komunikaty/artykuly-csirt-knf/362-ostrzezenia/887-wprowadzenie-do-sztucznej-inteligencji

- poruszamy w nim podstawy tematu sztucznej inteligencji, wychodząc od definicyjnego zrozumienia zagadnienia, poznania krótkiej historii oraz wyjaśnienia różnicy pomiędzy AI, ML i DL. Zachęcamy do zapoznania się z nim. Bez różnicy jednak na to, czym i jak działają przestępcy, to bardzo ważnym jest uczyć użytkowników Internetu, jak nie dać się złapać w sidła cyberprzestępców. A jedną z forma edukacji jest uświadamianie i informowanie. O bieżących schematach i scenariuszach przestępczych informujemy na naszych profilach w mediach społecznościowych: *X* (***Twitter***), ***LinkedIn*** oraz ***Facebook*** – zachęcamy do śledzenia i przekazywania dalej.

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: *https://www.linkedin.com/newsletters/biuletyn-nask-https://www.nask.pl/pl/aktualnosci/5166,Subskrybuj-Biuletyn-NASK-na-LinkedIn.html*

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*