



Ministerstwo
Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

10/2023





SPIS TREŚCI

<i>Rozwój Sztucznej Inteligencji: nowe możliwości i wyzwania</i>	<i>3</i>
<i>Haktywizm – narzędzie wojny informacyjnej w cyberprzestrzeni</i>	<i>4</i>
<i>Złośliwa niespodzianka – preinstalowane oprogramowanie w tanich urządzeniach z systemem Android.....</i>	<i>5</i>
<i>Atak Hamasu na Izrael zwiększył potencjał ataków hakerskich</i>	<i>6</i>
<i>Podatność w WinRAR w wersjach przed 6.23 – konieczna aktualizacja!.....</i>	<i>7</i>
<i>Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – ochrona klienta.....</i>	<i>8</i>
<i>INFORMACJA O SZKOLENIACH</i>	<i>10</i>
<i>Oznaczenia TLP.....</i>	<i>11</i>



Rozwój Sztucznej Inteligencji: nowe możliwości i wyzwania

Sztuczna inteligencja (AI) przekształca nasz świat w niespotykanych dotąd sposobie i tempie. Dzięki postępowi technologicznemu, AI staje się coraz bardziej zaawansowane, dostępne i szeroko wykorzystywane w procesach informacyjnych w warstwie technicznej rozwiązań IT, zwykle bez świadomości użytkowników o korzystaniu z technologii opartej o algorytmy AI. Szerokie grono użytkowników Internetu kojarzy AI wyłącznie z popularnymi *chatbotami* jak *Bard* czy *ChatGPT*. W ostatnich czasie, dwie firmy - *OpenAI* i *XAI* – upubliczniły kolejne narzędzia zwiększające dostępność rozwiązań w dziedzinie generatywnej sztucznej inteligencji.

OpenAI, znane z rozwoju modelu językowego *GPT*, wprowadziło niedawno nowy, bardziej zaawansowany model *GPT-4 Turbo*, który jest wydajniejszy i tańszy niż obecnie stosowane rozwiązania. Co szczególnie ważne, narzędzie te, umożliwi tworzenie niestandardowych wersji *ChatGPT* - *chatbotów* dostosowanych do własnych potrzeb, które można udostępniać innym, a nawet wykorzystywać do celów zarobkowych. Ponadto *OpenAI* udostępniła narzędzia służące dobru wspólnemu jak opracowana platforma *Codex*, która pozwala budować własne AI na bazie modelu *ChatGPT*, bez umiejętności kodowania. *Codex* może generować kod, tekst, grafikę, muzykę i inne rodzaje treści na podstawie prostych poleceń lub pytań.

Jednak rozwój AI napędzany jest również wysoką konkurencją podmiotów komercyjnych dążących do zbudowania własnej silnej pozycji w tym, dopiero tworzącym się rynku. Elon Musk, znany z innowacyjnego podejścia do technologii, niedawno zaprezentował swojego bota AI o nazwie *Grok* będącego konkurencją dla wymienionych wyżej *ChatGPT* oraz *Barda*. *Grok*, podobnie jak wspomniane rozwiązania jest zasilany przez zaawansowany model językowy (MML). *Grok* ma dostęp do danych gromadzonych przez serwis X (dawny *Twitter*) i ma na celu wspieranie ludzi i pomóc zrozumieć prawdziwą naturę wszechświata.



Logotyp firmy Grok. Źródło: x.ai

W opinii przedstawicieli firmy, *Grok* ma być przyjaznym i pomocnym asystentem domowym, ale także ma się cechować sarkastycznym poczuciem humoru przy zapewnieniu wysokiej efektywności i precyzji generowanych treści, przy niższym od konkurencyjnych rozwiązań zużyciu zasobów energetycznych i technicznych.

Mimo wszystko AI nie jest pozbawiona kontrowersji i wyzwań. Podczas październikowego szczytu dot. AI w brytyjskim Bletchley Park część ekspertów i przedsiębiorców, w tym Elon Musk ostrzegali przed potencjalnymi, dalekosiężnymi zagrożeniami związanymi z AI, zaliczyli do nich m. in.: perspektywę masowych zwolnień, utratę kontroli nad algorytmami, utratę prywatności czy w konsekwencji... utratę sensu życia. E. Musk twierdzi, że AI może być niebezpieczna dla ludzkości, jeśli nie będzie odpowiednio regulowana i nadzorowana. Rozwój AI otwiera nowe możliwości i stawia wyzwania, wymagając skutecznego zarządzania ryzykiem i wykorzystania jej potencjału. Ewolucja algorytmów generatywnych AI jak *Bard*, *ChatGPT* i *Grok*, pokazują postęp oraz zwracają uwagę na konsekwencje, podkreślając potrzebę zrównoważonego rozwoju i odpowiedzialnego wykorzystania AI. Przedstawiciele G7 oraz UE zapewnili, że są świadomi ww. zagrożeń i wyzwań oraz, że takie regulacje wkrótce nastąpią, co koresponduje z próbami prawnego uregulowania AI w USA oraz krajach wschodniej Azji.

Źródła: x.ai, itwiz.pl, rp.pl



Haktywizm – narzędzie wojny informacyjnej w cyberprzestrzeni

Obecne konflikty międzynarodowe nie ograniczają się wyłącznie do fizycznego pola bitwy. Obejmują one również cyberprzestrzeń, gdzie hakywiści wykorzystują techniki hakerskie do realizacji nie tylko swoich celów politycznych i społecznych, ale również z zamiarem osiągnięcia zakładanych celów w obszarach psychologicznych i socjologicznych w sferze informacyjnej.



Rosyjscy hakywiści. Źródło: cnc.com

Haktywizm narodził się w latach 80. XX w. Zyskał szczególną sławę za sprawą grup *Anonymous*. W ostatnich latach haktywizm wyraźnie ewoluował. Ugrupowania przyjmują wartości typowe dla tradycyjnego aktywizmu obywatelskiego, jak nieograniczona wolność wypowiedzi, radykalizm religijny, anarchizm, ekstremizm, wspieranie lokalnych opozycji politycznych czy stron konfliktów

zbrojnych. Ostatnio obserwowana dynamika starć politycznych i zbrojnych, przy panującym wszechobecnym środowisku sieciowym spowodowała, że haktywizm stał się nieoficjalnym narzędziem projekcji siły i realizacji interesów przez agendy państwowe odpowiedzialne za działania w cyberprzestrzeni.

Na przykładzie konfliktu rosyjsko-ukraińskiego, specjaliści stwierdzają się, że rosyjskojęzyczne grupy haktywistyczne służą jako maskowanie (głównie medialne) dla wyrafinowanych i zaawansowanych technicznie działań grup APT (*Advanced Persistent Threat*). Ponadto zakłada się, że grupy haktywistyczne są bezpośrednio związane z grupami APT oraz tak jak one, podlegają nadzorze, kontroli i finansowaniu przez służby specjalne Federacji Rosyjskiej (FR). Od czasu rosyjskiej inwazji na Ukrainę zauważa się gwałtowny wzrost aktywności rosyjskich ugrupowań. Grupy takie jak m.in. *KillNet*, *Beregini* i *NoName057* systematycznie przeprowadzają ataki typu *DDoS*, wyciek danych (*data leaks*), niszczenie infrastruktury sieciowej (*Web Defacement*) oraz ransomware. Dodatkowo zauważa się tzw. *operacje pod fałszywą flagą* prowadzone z zamiarem dyskredytacji nieprzyjaznych i konkurencyjnych grup hakerskich.

Celem wspomnianych ataków są organizacje oraz podmioty państwowe i prywatne na Ukrainie oraz w krajach zachodnich, w tym w Polsce. Hakywiści informują o prowadzonych działaniach w sposób hiperboliczny i wyidealizowany na swoich kanałach na *Telegramie*. Mimo krótkotrwałych zaburzeń działania atakowanej infrastruktury, ataki te posiadają wyraźne znaczenie medialne w ramach prowadzonej wojny informacyjnej, szczególnie w zakresie propagandy i dezinformacji. Powyższe skutki mają przede wszystkim wydźwięk społeczny i wpływają na polaryzację społeczeństw oraz tworzą oddolne poparcie dla ultra-wolnościowych, antysystemowych i antyestablishmentowych idei, które dani hakywiści reprezentują, co zwykle okazuje się wsparciem realizacji interesów informacyjnych FR.

Podsumowując, haktywizm ewoluuje i zyskuje na znaczeniu jako narzędzie walki w przestrzeni cyfrowej. W obliczu rosnącej aktywności grup haktywistycznych, konieczne jest zrozumienie głównego celu ich działalności oraz przeciwdziałanie wykorzystywanym przez nie technikom i taktykom. Haktywizm jest nie tylko narzędziem walki, ale także środkiem do manipulowania i wpływania na opinię publiczną. Zrozumienie i przeciwdziałanie haktywizmowi jest niezbędne dla utrzymania bezpieczeństwa i stabilności w dzisiejszym cyfrowym świecie.

Źródła: *socradar.io*, *flashpoint.io*



Złośliwa niespodzianka – preinstalowane oprogramowanie w tanich urządzeniach z systemem Android

Zakup taniego urządzenia z *Androidem* może być kosztownym błędem, zwłaszcza jeżeli jest zainfekowane wirusami już w momencie wyjęcia nowego urządzenia z pudełka. Analitycy cyberbezpieczeństwa uważają, że co najmniej 74 tys. urządzeń z *Androidem* tj. telefonów komórkowych, tabletów, urządzeń *Connected TV* itp. mogło zostać zainfekowanych preinstalowanym złośliwym oprogramowaniem, jako część sieci *BADBOX*, które zostało załadowane na etapie produkcji. Mamy w tym przypadku do czynienia ze skompromitowanym łańcuchem dostaw sprzętu.



Logo android. Źródło: android.com

Produkty zawierające złośliwy backdoor zostały znalezione w sieciach szkół publicznych w całych Stanach Zjednoczonych. Zespół analityków z *Human Security* zidentyfikował łańcuch dostaw chińskiego producenta, który został naruszony w celu włamania się do oprogramowania kilku produktów dostarczanych do sprzedawców, fizycznych sklepów detalicznych i magazynów e-commerce. Backdoor oprogramowania układowego był oparty na złośliwym oprogramowaniu *Triada*, które zostało było znajdowane na przestrzeni lat w tanich smartfonach z *Androidem*. „Niestety, urządzenia zainfekowane *BADBOX* są nie do naprawienia przez przeciętnego użytkownika. Ponieważ złośliwe oprogramowanie znajduje się na partycji tylko do odczytu (ROM) oprogramowania układowego urządzenia, przeciętny użytkownik nie będzie w stanie usunąć *BADBOX* ze swojego produktu.”

Nie tylko tanie urządzenia mogą być źródłem problemów. Podatności i błędy w systemie wykrywane są również regularnie w sprzęcie dużych dostawców takich jak *Samsung*, czy *Apple*. Dla przykładu firma *Apple* w październiku ujawniła i załatała 2 luki typu zero-day (17 luka w 2023 r.), które są aktywnie wykorzystywane, śledzone jako CVE-2023-42824 (możliwa eskalacja uprawnień na zainfekowanych urządzeniach) i CVE-2023-5217 (podatność związana z przepełnieniem bufora w kodowaniu VP8 biblioteki kodeków video libvpx, co może umożliwić atakującemu wykonanie dowolnego kodu). Na chwilę obecną dostępna jest najnowsza aktualizacja iOS 17.1.1.



Logo Apple. Źródło: apple.com

Rekomendacje: Użytkownicy powinni pamiętać o regularnych aktualizacjach sprzętu. Zawierają one ważne poprawki błędów i zapobiegają wykorzystaniu znanych podatności w systemach. Przy zakupie sprzętu wybieraj marki, które istnieją od dłuższego czasu i są aktywnie sprzedawane w wielu krajach. Jeśli masz okazję zobaczyć urządzenie w sklepie, zrób to. Tam przejdź do ustawień i sprawdź, czy istnieje opcja instalacji aktualizacji. Sprawdź też jaką wersję systemu ma zainstalowany telefon. Wszystko poniżej wersji 12 w przypadku Androida można uznać za przestarzałe. Ponadto przeczytaj opinie kupujących na specjalistycznych forach - nie na platformach handlowych lub stronach internetowych sklepów. Natychmiast po zakupie urządzenia zapoznaj się z jego ustawieniami, zaktualizuj oprogramowanie do najnowszej wersji, a następnie odinstaluj lub wyłącz za pomocą ustawień wszystkie aplikacje, które wydają się zbędne.

Źródła: zdnet.com, recordedfuture.com, darkreading.com, humansecurity.com

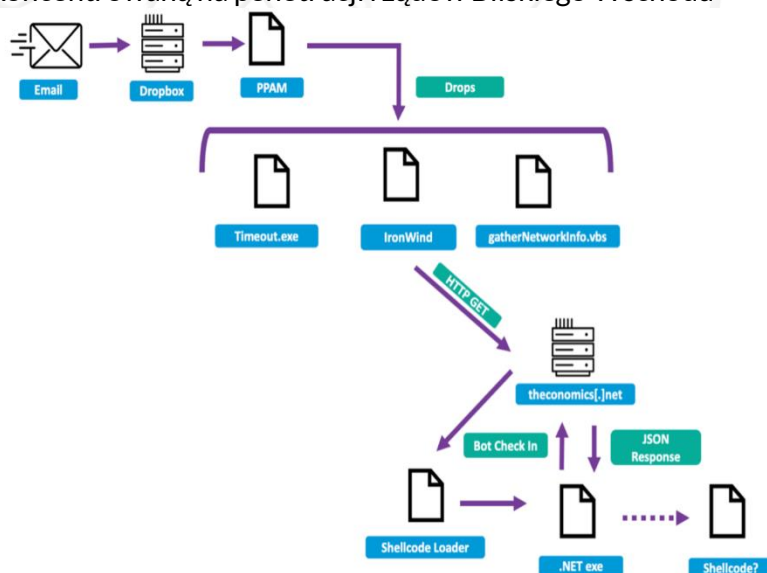


Atak Hamasu na Izrael zwiększył potencjał ataków hakerskich

Rankiem 7 października 2023 r. Hamas przeprowadził wielopłaszczyznowy atak kinetyczny na cele cywilne i wojskowe w środkowym i południowym Izraelu. Analitycy cyberbezpieczeństwa śledzą aktywność grup hakerskich działających na rzecz Palestyny wśród których jedna z najaktywniejszych to *Molerats* (*Gaza Cybergang*, *Gaza Hacker Team*, *TA402*, *Frankenstein*, *WIRTE*).

Grupa ma na celowniku głównie podmioty rządowe (w tym placówki dyplomatyczne), finansowe, wojskowo-polityczne działające lub realizujące interesy na terytoriach Palestyny. Są to przede wszystkim ministerstwa spraw zagranicznych, zagraniczne misje w Palestynie i podmioty rządowe na Bliskim Wschodzie. Grupa w ostatnim miesiącu realizowała wysoce skoncentrowane kampanie phishingowe, przy czym wykorzystuje złożone łańcuchy infekcji złośliwym oprogramowaniem. Nie jest jasne kim są hakerzy powiązani z grupą, lecz w ostatnich latach badacze opisali ją jako skoncentrowaną na penetracji rządów Bliskiego Wschodu i zbieraniu wszelkich informacji dot. Palestyny.

W połowie 2023 r. badacze z firmy *Proofpoint* po raz pierwszy zidentyfikowali aktywność *Molerats* wykorzystującą labiryntowy łańcuch infekcji do atakowania rządów Bliskiego Wschodu za pomocą nowego programu do ustanawiania wstępnego dostępu, który *Proofpoint* nazwał *IronWind*. Od lipca do października 2023 r.



Łańcuch infekcji użyty w kampanii w lipcu 2023 r. Źródło: proofpoint.com

Molerats wykorzystywał trzy warianty tego łańcucha infekcji - łączyła *Dropbox*, załączniki plików XLL i załączniki plików RAR - przy czym każdy wariant konsekwentnie prowadził do pobrania biblioteki DLL zawierającej wielofunkcyjne złośliwe oprogramowanie. *Molerats* odszedł również od korzystania z usług w chmurze, takich jak *Dropbox API*, które analitycy zaobserwowali w aktywności z lat 2021 i 2022, na rzecz wykorzystania infrastruktury kontrolowanej przez adversarza do C2.

Zaobserwowano bardziej zaawansowane łańcuchy infekcji, które wskazują na ewolucję grupy i stosowanych przez nią metod. Grupa *Molerats* pozostaje trwałym zagrożeniem, przekształcając swoje metody ataku i dostarczania złośliwego oprogramowania w celach cyberszpiegowskich - dążąc do gromadzenia jak największej ilości danych wywiadowczych.

Źródła: malware.news, infosecurity-magazine.com, cyberscoop.com, Recorded Future, proofpoint.com



Podatność w WinRAR w wersjach przed 6.23 – konieczna aktualizacja!

W ostatnim czasie aktywnie wykorzystywana jest podatność, **CVE-2023-38831** w WinRAR, który jest popularnym narzędziem do archiwizacji plików dla systemu Windows.

Cyberprzestępcy eksplorowali lukę od początku 2023 r. celem ataków instytucje rządowe.

WinRAR w wersji wcześniejszej niż 6.23 posiada lukę pozwalającą atakującym na wykonanie dowolnego kodu, gdy użytkownik próbuje wyświetlić nieszkodliwy plik (taki jak zwykły .png, czy .jpg) w archiwum ZIP. Gdy użytkownik dwukrotnie kliknie na plik "poc.png_" (*podkreślenie jest używane do wskazania spacji*) z interfejsu użytkownika WinRAR, WinRAR w wersji przed 6.23 zamiast tego wykona "poc.png_/poc.png_.cmd".

Po dwukrotnym kliknięciu pliku przez użytkownika, WinRAR próbuje określić, które pliki muszą zostać tymczasowo rozszerzone, iterując po wszystkich wpisach archiwum. Jednak ze względu na sposób dopasowywania, jeśli zostanie znaleziony katalog o tej samej nazwie co wybrany wpis, zarówno wybrany plik, jak i pliki wewnątrz dopasowanego katalogu zostaną wyodrębnione do katalogu głównego losowego katalogu tymczasowego (TEMP). Podczas zapisywania zawartości plików WinRAR wykonuje normalizację ścieżki, która usuwa dołączone spacje, ponieważ system Windows nie zezwala na pliki z końcowymi spacjami.

Na koniec WinRAR wywołuje:

- `ShellExecuteExW`, przekazując nieznormalizowaną ścieżkę z końcową spacją do `"%TEMP%\{losowy_katalog}\poc.png_"`, aby uruchomić plik.
- Następnie, wewnętrznie `ShellExecute` próbuje zidentyfikować rozszerzenia plików poprzez wywołanie `"shell32!PathFindExtension"`, co kończy się niepowodzeniem, ponieważ rozszerzenia ze spacjami są uważane za nieprawidłowe.
- W dalszej kolejności, `ShellExecute` wywołuje `"shell32!ApplyDefaultExts"`, które iteruje przez wszystkie pliki w katalogu, znajdując i wykonując pierwszy plik z rozszerzeniem pasującym do któregośkolwiek z zakodowanych na stałe: .pif, .com, .exe, .bat, .lnk, .cmd. Tym sposobem uruchamia się proces i pobierane jest złośliwe oprogramowanie na komputer ofiary, które może zostać dostarczone przez adversarza np. z wykorzystaniem reverse proxy ustanowionym na zasobie chmurowym wybranego dostawcy, które z kolei może mieć połączenie bezpośrednie lub pośrednie z serwerem C2.



Opracowanie własne – uproszczony schemat infrastruktury atakującego z wykorzystaniem usługi Ngrok – jako reverse proxy.

Rekomendacje: Użytkownicy WinRAR powinni jak najszybciej przeprowadzić aktualizację do najnowszej wersji 6.24 dostępnej na stronie: [WinRAR archiver, a powerful tool to process RAR and ZIP files \(rarlab.com\)](https://www.rarlab.com).

Źródła: cve.mitre.org, blog.google, [Recorded Future](https://RecordedFuture.com), rarlab.com



Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – ochrona klienta

W październiku 2023 r. do blokady zgłosiliśmy 3 203 domeny, które przeanalizowaliśmy i 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.).

Październik to kolejny miesiąc, w którym cyberprzestępcy podszywając się pod znane osoby lub instytucje, starali się nakłonić ofiary do rzekomego inwestowania środków. Zauważamy jednak, że coraz częściej przestępcy w fałszywych ofertach wykorzystują motyw związany ze sztuczną inteligencją. Dlaczego? Ponieważ jest to temat na który coraz częściej dyskutuje się w przestrzeni publicznej, a jednocześnie to obszar dynamicznie się rozwijający i trudno śledzić go całkowicie na bieżąco. To sprawia, że jest on wdzięcznym motywem dla scenariuszy przestępczych. Wracając jednak do „fałszywych inwestycji”, to po kliknięciu w link we wspomnianej wcześniej reklamie, klient trafia na stronę, na której wymagane jest dokonanie rzekomej rejestracji. Dane pozyskane przez cyberprzestępców w ten sposób umożliwiały im nawiązanie kontaktu z potencjalną, już zmanipulowaną osobą, a w kolejnym kroku kradzież jej środków. Niejednokrotnie, w podobnych przypadkach, przestępcy zachęcali do instalowania oprogramowania do zdalnej obsługi lub połączenia się przez usługę udostępniania pulpitu w komunikatorze Whatsapp. W momencie, kiedy ofiara tego przestępstwa chce wypłacić rzekomo zarobione środki (często orientując się, że mogła zostać oszukana) otrzymuje informację o konieczności „sprawdzenia konta bankowego poprzez system AML”. W tym celu cyberprzestępcy przekazują link do strony phishingowej, na której wyłudzane są dane uwierzytelniające do bankowości elektronicznej. I tym sposobem cyberprzestępcy najpierw nakłaniają ofiarę do przekazywania wysokich kwot, a następnie pozyskują dostęp do bankowości elektronicznej. W ostatnim czasie rozszerzyli jednak swój wariant oszustwa. W publikowanych fałszywych reklamach oferowali pomoc w odzyskaniu środków osobom, które padły już wcześniej ofiarami fraudu inwestycyjnego. Wszystko po to, aby dalej prowadzić grę psychologiczną i nakłaniać do zainwestowania kolejnych pieniędzy. Oprócz tego cyberprzestępcy publikowali reklamy, w których oferowali produkty w konkurencyjnych cenach. Na stronach phishingowych podszywali się pod sklep MOHITO, CROPP, EOBUIE oraz SINSAY. Po wejściu na stronę, ofiara musiała wypełnić formularz osobowy, a następnie zachęcana była do wpisania danych karty płatniczej. W ten sposób dane te trafiały w ręce przestępców. Ciekawym i dawno nieidentyfikowanym scenariuszem było podszywanie się pod Polskie Linie Lotnicze LOT. Atakujący ogłosili rzekomą możliwość zakupu zagubionych bagaży. Po kliknięciu w reklamę na platformie Facebook, ofiara trafiała na stronę phishingową, na której wymagane było wprowadzenie danych karty płatniczej. Na tapetę przestępczą poszedł również ZTM (Zarząd Transportu Miejskiego w Warszawie). Cyberprzestępcy ogłosili rzekomą możliwość zdobycia karty uprawniającej do przejazdów, w bardzo atrakcyjnej cenie. Po kliknięciu w link z reklamy, ofiara trafiała na stronę phishingową, na której informowana była o losowaniu. Oczywiście „wygrywała”, a w następnym kroku, poszkodowany przekierowywany był na stronę, gdzie kazano mu wpisać dane osobowe oraz dane karty płatniczej. Również znane wcześniej, ale niemniej groźne były kampanie w których atakujący publikowali posty na portalu Facebook, zawierające sensacyjne informacje. Po wejściu w taką informację użytkownik trafiał na stronę z rzekomym artykułem, na której, aby możliwe było



zapoznanie się z jego treścią, należało potwierdzić swój wiek poprzez zalogowanie się do konta w mediach społecznościowych. Ofiara wprowadzając swoje poświadczenia logowania na niebezpiecznej stronie pozwalała oszustom na przejęcie jej konta. Cyberprzestępcy mogli publikować w imieniu ofiary kompromitujące treści lub wysyłać wiadomości do jej znajomych w celu wyłudzenia pieniędzy. Rzecz jasna, w październiku 2023 r., nie zabrakło również SMS-ów podszywających się pod polskie banki i informujących o np. rzekomej blokadzie dostępu do bankowości, czy fałszywych wiadomości e-mail straszących przed konsekwencjami (np. blokada dostępu do Netflix), jeżeli nie kliknie się w załączony link i nie wykona podanych na stronie phishingowej kroków. Wszystkie te działania miały jednak na celu jedno – wyłudzenie takich danych, by móc je wykorzystać do wyprowadzania środków w rachunku ofiary. Niejednokrotnie wysokich kwot, a nawet wpędzania ludzi w ogromne zadłużenia.

Jak może przeczytać wyżej, październik to kolejny miesiąc, który udowodnił, że przestępcy nieustannie udoskonalają swoje sposoby działania. Niezmiennie uważamy, że ważnym jest, aby



Business E-mail Compromise

Złośliwe aplikacje mobilne

Media społecznościowe

Scam "na kupującego"

Przykładowe scenariusze przestępcze opublikowane na stronie CEBRF

przewodzić działania informacyjne i edukacyjne - do czego wszystkich zachęcamy. Jednocześnie informujemy, że w minionym miesiącu zakończyliśmy publikację cyklu #TwojeCyberbezpieczeństwo, w ramach którego stworzyliśmy 11 najczęściej występujących schematów oszustw internetowych (rysunek). Opisywaliśmy w nich jak przebiegają poszczególne przestępstwa oraz jak można się przed nim uchronić. Wszystkie opublikowane zostały na naszej stronie: <https://cebrf.knf.gov.pl/encyklopedia-cyberbezpieczenstwa/schematy-oszustw> - zachęcamy do zapoznania się z nimi i przekazania dalej, a także śledzenia nas w mediach społecznościowych, gdzie na bieżąco staramy się umieszczać informacje o schematach i scenariuszach przestępczych oraz ostrzegać przed trwającymi w danym momencie kampaniami phishingowymi: X (Twitter), LinkedIn oraz Facebook.



INFORMACJA O SZKOLENIACH

Zachęcamy również do udziału w bezpłatnych szkoleniach online dla podmiotów krajowego systemu cyberbezpieczeństwa, które organizuje Departament Cyberbezpieczeństwa MC.

Wszystkie informacje na temat szkoleń (w tym harmonogram i formularze zgłoszeń) znajdują się na stronie internetowej bazy wiedzy cyberbezpieczeństwa na portalu gov.pl – pod linkiem: <https://www.gov.pl/web/baza-wiedzy/szkolenia>

Zachęcamy również do zasubskrybowania biuletynu NASK – jest to przegląd najważniejszych informacji nt. cyberbezpieczeństwa, edukacji cyfrowej i nowych technologii.

Link do zapisów:

<https://www.nask.pl/pl/aktualnosci/5166,Subskrybuj-Biuletyn-NASK-na-LinkedIn.html>



Źródło: <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 konsultantów) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań. Dodatkowo 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 informacjami 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