



Ministerstwo
Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

07/2023





Megakonstelacje na orbicie: rozwój technologii satelitarnych.....	3
Rosyjscy hakerzy powiązani z grupą APT29 celują w organizacje rządowe atakami phishingowymi z wykorzystaniem <i>Microsoft Teams</i>	4
Maile w niepowołanych rękach na skutek literówek.....	5
Adminie, instaluj aktualizacje – kasus Fortinet	6
Nowe inicjatywy NASK: Firma Bezpieczna Cyfrowo i CVE.....	7
<i>Apple</i> aktywnie zwalcza cyberzagrożenia w swoich produktach.....	8
<i>WormGPT</i> - AI w rękach cyberprzestępców.....	9
Kampanie przestępcze w lipcu 2023 oczami CSIRT KNF.....	10
INFORMACJA O SZKOLENIACH.....	13
Oznaczenia TLP.....	14



Megakonstelacje na orbicie: rozwój technologii satelitarnych

Jedną z bardziej rozpoznawalnych nazw jest *Starlink*, projekt satelitarny firmy *SpaceX*. Jest to rozbudowana sieć niewielkich satelitów umieszczonych na niskiej orbicie okołoziemskiej mających na celu dostarczanie szerokopasmowego Internetu na całym świecie. Ma to duże znaczenie w przypadku pokrycia miejsc, gdzie tradycyjne usługi internetowe są trudne do zrealizowania, takich jak tereny odległe np. morskie. Polska jest jednym z większych dostawców systemów *Starlink* na Ukrainę, przekazując tysiące sztuk. Nowoczesny sprzęt satelitarny umożliwia komunikację z dowolnego miejsca na Ukrainie, niezależnie od infrastruktury naziemnej, która jest tam dostępna. Ponadto Polska wysłała w ostatnim czasie również 500 akumulatorów *Tesla Powerwall*, które oprócz dostarczania energii do szkół, szpitali, czy przedszkoli, wspomogą w nieprzerwanym działaniu systemu *Starlink* w wybranych, trudniej dostępnych lokalizacjach.

Warto mieć na uwadze rozwój tego typu projektów również przez Chiny i Rosję. W przypadku Chin, rząd zatwierdził krajowy plan budowy megakonstelacji *Guowang* w 2021 r., obejmujący 13 000 satelitów. Chiny równolegle prowadzą drugi projekt budowy szerokopasmowej megakonstelacji znany jako „*G60 Starlink*”. Przewiduje on budowę konstelacji na ponad 12 000 satelitów, przy czym eksperymentalne satelity już zostały wystrzelone i połączone w sieć. Rosja, a dokładniej rosyjska agencja kosmiczna *Roskosmos* od 2018 r. realizuje zapowiedziany przez Władimira Putina projekt „*Sfera*”. Projekt wielofunkcyjnej satelitarnej konstelacji pierwotnie zakładał 640 satelitów do 2030 r., obecnie nie wiadomo na jakim jest etapie.



Interaktywna mapa pokrycia *Starlink*, <https://www.starlink.com/map>

Programów kosmicznych realizowanych przez różne państwa i organizacje jest wiele, tak w zakresie łączności satelitarnej, jak i innych zdolności kosmicznych, jak np. rozpoznawanie obrazowe i radarowe, czy PNT (*Position, Navigation, and Timing*). *SpaceX* nadal rozszerza swoją konstelację o nowe warianty *Starlink*. firma *Amazon* realizuje „*Project Kuiper*”, a UE chce stworzyć własny system satelitarny do 2027 r – *Iris 2*. Ponieważ przestrzeń kosmiczna staje się coraz bardziej zatłoczona, kraje i przedsiębiorstwa muszą wziąć pod uwagę długoterminowy pakt na rzecz środowiska i zagrożenia związane z rozprzestrzenianiem satelitów.

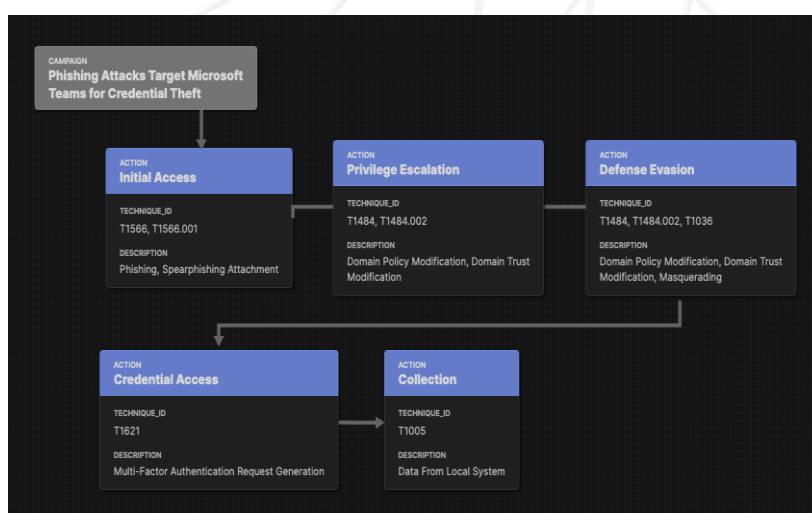
Źródła: pulskosmosu.pl, telepolis.pl, rp.pl, spacevoyaging.com, money.pl



Rosyjscy hakerzy powiązani z grupą APT29 celują w organizacje rządowe atakami phishingowymi z wykorzystaniem *Microsoft Teams*

Ataki phishingowe były realizowane przez śledzoną przez *Microsoft* grupę *Midnight Blizzard* (NOBELIUM) w celu kradzieży danych uwierzytelniających za pośrednictwem czatów *Microsoft Teams*. Podejrzewa się że grupa powiązana jest z rosyjską Służbą Wywiadu Zagranicznego. Celem grupy jest zbieranie danych wywiadowczych poprzez zastosowanie różnych technik szpiegowskich obserwowanych od 2018 r. Działania często wiążą się z naruszeniem bezpieczeństwa istotnych kont w tym z zastosowaniem zaawansowanych technik łamania mechanizmów uwierzytelniania w organizacji celem rozszerzenia dostępu i uniknięcia wykrycia.

Raport *Microsoft Threat Intelligence* z 2 sierpnia 2023 r. ujawnia, że celem kampanii było około 40 globalnych organizacji, przy czym koncentrowano się m.in na sektorze rządowym, organizacjach pozarządowych, usługach IT, sektorze technologii. Atak rozpoczął się gdy hakerzy uzyskali dostęp do dzierżaw platformy *Microsoft 365* (tenants). Następnie wykorzystano zainfekowane konta, których właścicielami były głównie mniejsze firmy do utworzenia nowych domen, które wyglądały na legalne. Cyberprzestępcy wykorzystali nowo utworzone domeny do wysyłania wiadomości phishingowych za pośrednictwem *Microsoft Teams*, podszywając się pod zespół pomocy technicznej firmy *Microsoft*. Wiadomości phishingowe zostały wysłane z legalnej domeny onmicrosoft.com, co spowodowało że wyglądały na autentyczne. Głównym celem tych wiadomości było nakłonienie ofiar do ujawnienia danych logowania oraz autoryzacja monitów o uwierzytelnienie wieloskładnikowe (MFA). Po uzyskaniu dostępu hakerzy mogli przejąć pełną kontrolę nad zaatakowanymi kontami, co doprowadziło do wydobycia poświadczeń użytkownika i informacji z dzierżawy platformy *Microsoft 365*.



Opracowanie własne na podstawie pozyskanych informacji (MITRE ATT&CK)

Więcej na temat ataku można przeczytać na stronie: <https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/>

Źródła: *Microsoft.com, attack.mitre.org, Recorded Future, mitre-engenuity.org*



Maile w niepowołanych rękach na skutek literówek

W wyniku literówek w adresie email przez lata miliony maili kierowanych do amerykańskiego wojska, które posiada domenę .mil, były wysyłane na adresy z końcówką .ml, która jest domeną najwyższego poziomu Mali. Do przypadkowych adresatów trafiać miały wiadomości zawierające m.in. dane medyczne, dokumenty tożsamości, mapy instalacji wojskowych, plany podróży, rezerwacje dla wysokich rangą dowódców wojskowych.

Nie wszystkie maile dotarły do skrzynek w domenę .ml, gdyż jeśli nie istnieje odpowiednia skrzynka pocztowa w domenę .ml odpowiadająca skrzynce pocztowej w domenę .mil, wiadomość nie zostanie dostarczona. Jednakże firma Mali Dili, która zarządza domeną krajową .ml, po zauważeniu dużej liczby żądań DNS dla malijskich domen, które nie istniały, skonfigurowała system przechwytywania. W wyniku szybkiego przeciążenia systemu firma wkrótce przestała przechwytywać pocztę. Twierdzi też, że wielokrotnie próbowała zaalarmować rząd amerykański o tej sprawie, ale bez powodzenia.

W 2023 r. Mali Dili ponownie zaczęło zbierać źle kierowane maile, aby - jak twierdzi - pokazać je władzom USA. Miało ich się zbierać blisko 120 tys. Departament Obrony USA poinformował, że wdrożył środki techniczne, które uniemożliwiają użytkownikom wysyłanie niewłaściwych maili poprzez ich blokowanie, zanim opuszczą one systemy resortu obrony. Problemem pozostają wiadomości wysyłane z podmiotów zewnętrznych do amerykańskiego wojska, np. z biur podróży, które obsługują wyjazdy służbowe Pentagonu. Należy także zauważyć, że po wygaśnięciu umowy z Mali Dili, malijski rząd, który współpracuje z Rosją, będzie mógł przejąć wysyłane maile.

Rekomendacje: podobno pomyłki zdarzają się też w innych krajach (np. mylenie domen nl i .ml), sytuacje takie mogą występować również w Polsce. Nawet jeśli rzadziej z uwagi na brak podobnych nazw domen, to jednak nawet nieliczne wiadomości błędnie wysłane mogą zawierać wrażliwe informacje lub dane osobowe. W przypadku zaobserwowania w danej organizacji tego typu sytuacji należy wdrożyć środki techniczne, które będą blokować błędnie zaadresowane maile (co pozwoli ograniczyć przynajmniej przypadkową korespondencję kierowaną na zewnątrz). Istnieje też ryzyko, że grupy przestępcze lub obce służby mogą rejestrować domeny o podobnych nazwach, aby przechwytywać wiadomości (np. administracji rządowej i infrastruktury krytycznej). Dlatego też warto rozważyć włączenie tej tematyki do szkoleń z cyber higieny, aby uwrażliwić pracowników na możliwość wycieku spowodowanego literówką.

Źródła: TheRegister.com.



.ml



.mil

Godło Mali i logo
Departamentu Obrony



Adminie, instaluj aktualizacje – kazu Fortinet

W czerwcu br. ujawniano krytyczną podatność CVE-2023-27997 w sprzęcie sieciowym firmy Fortinet, jednego z głównych dostawców firewalle i VPN, umożliwiającą przeprowadzenie cyberataków¹. Firma udostępniła aktualizację, która łąta tę poważną lukę, jednak badacze wskazują, że spośród 489 337 urządzeń podłączonych do Internetu, których dotyczy ten problem, prawie 336 000 pozostawało narażonych na tę krytyczną podatność (69%), gdyż administratorzy nie zainstalowali poprawek (według stanu na początek lipca, tj. trzy tygodnie po opublikowaniu aktualizacji).

Zwrócono także uwagę, że na podstawie danych z *Sohadana* (wyszukiwarka pozwalająca na skanowanie różnych urządzeń i systemów), niektóre z podatnych na ataki urządzeń działa oprogramowanie *Fortigate*, które nie było aktualizowane od 2015 roku!

```
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.250.124 - - [21/Jun/2023 11:21:57] "GET /busybox HTTP/1.1" 200 -

Listening on 0.0.0.0 1337
Connection received on 192.168.250.124 18578
id
uid=0 gid=0
grep config-version /data2/config/cfg*
/data2/config/cfg0000000001:#config-version=F
GVM64-7.2.4-FW-build1396-230131:opmode=0:vdom
=0:user=daemon_admin
/data2/config/cfg0000000002:#config-version=F
GVM64-7.2.3-FW-build1262-221109:opmode=0:vdom
=0:user=daemon_admin
/data2/config/cfg0000000003:#config-version=F
GVM64-7.2.4-FW-build1396-230131:opmode=0:vdom
=0:user=daemon_admin
[P0C] 0:CVE-2023-27997*
```

Zrzut ekranu z exploita do testowania urządzeń Fortinet opracowany przez firmę Bishop Fox
Źródło <https://arstechnica.com/security/2023/07/336000-servers-remain-unpatched-against-critical-fortigate-vulnerability/>

Nie jest to pierwsza luka w urządzeniach Fortinet, którą wykorzystują cyberprzestępcy. Przykładowo, w grudniu ubiegłego roku nieznani aktorzy wykorzystali inną krytyczną lukę w FortiOS SSL-VPN, aby zainfekować organizacje rządowe i powiązane z rządem zaawansowanym złośliwym oprogramowaniem stworzonym na zamówienie.

Rekomendacje: brak aktualizacji firewalle i innych urządzeń stanowi poważne zagrożenie dla cyberbezpieczeństwa organizacji. Niezałatane luki mogą skutkować incydentami, np. skutkującymi wykradzeniem informacji lub zaszyfrowaniem danych. Administratorzy systemów powinni dbać o aktualność oprogramowania, w tym sprzętowego, poprzez niezwłoczne instalowanie łatek udostępnianych przez producenta.

Źródła: ArsTechnica.com

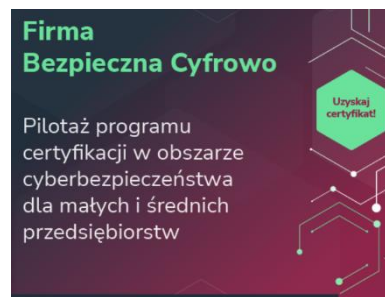
¹ Analiza podatności dostępna jest na stronie Fortinet: <https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign>



Nowe inicjatywy NASK: Firma Bezpieczna Cyfrowo i CVE

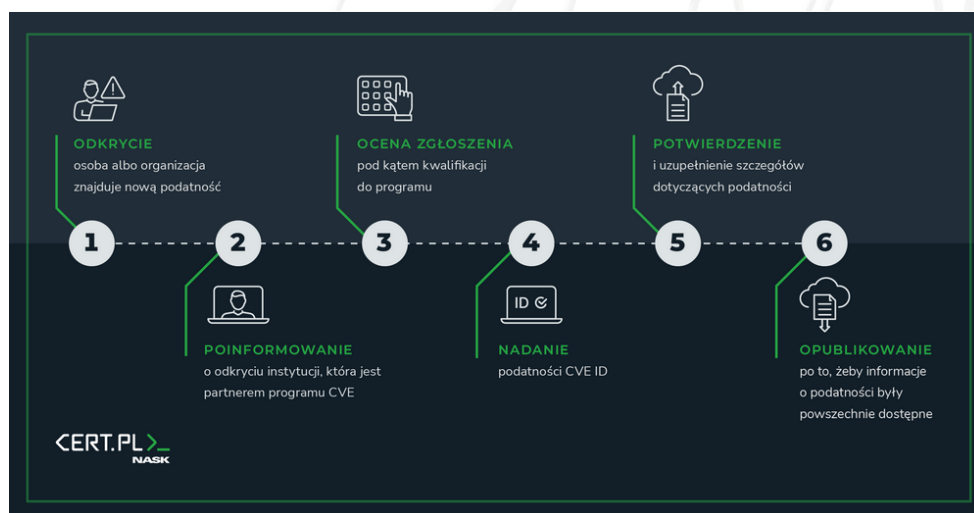
Państwowy Instytut Badawczy NASK wystartował z nowym programem Firma Bezpieczna Cyfrowo, którego celem jest rozwój kompetencji cyfrowych wśród polskich przedsiębiorców, podniesienie poziomu ochrony sieciowej w sektorze małych i średnich przedsiębiorstw (MŚP) i stabilności obrotu gospodarczego w kraju, a także upowszechnienie i wdrożenie nowego standardu cyberbezpieczeństwa w firmach. Jest to inicjatywa pilotażowa przygotowana wspólnie przez NASK wraz z Ministerstwem Rozwoju i Technologii oraz Ministerstwem Cyfryzacji.

Firmy biorące udział w programie będą mogły otrzymać certyfikat wydawany przez Jednostkę Certyfikującą NASK. Więcej informacji na stronie: <https://www.nask.pl/pl/aktualnosci/5213,Firma-Bezpieczna-Cyfrowo-startuje-nowy-program-edukacji-i-certyfikacji-cyber-bezp.html>



Zródło <https://www.nask.pl/pl/aktualnosci/5213,Firma-Bezpieczna-Cyfrowo-startuje-nowy-program-edukacji-i-certyfikacji-cyber-bezp.html>

Kolejny sukces NASK miał miejsce na arenie międzynarodowej. Zespół CERT Polska działający w strukturach NASK od początku sierpnia br. jako jedyna instytucja w Polsce i jeden z 7 CERT-ów w Europie może nadawać numery CVE (Common Vulnerabilities and Exposures), które służą do identyfikacji i katalogowania publicznie ujawnionych podatności. CVE to międzynarodowy program wspierający ujawnianie luk bezpieczeństwa w oprogramowaniu. Każda osoba, która znajdzie podatność może zgłosić ją do organizacji będącej CNA, czyli CVE Numbering Authority. Są to organizacje, które oceniają zasadność zgłoszenia, nadają podatnościom numery i dbają o jakość bazy. Baza CVE jest publiczna i dostępna za darmo. Jest ona podstawą dla organizacji z całego świata przy identyfikacji i śledzeniu informacji o nowych lukach bezpieczeństwa. Dowiedz się więcej na stronie NASK: <https://www.nask.pl/pl/aktualnosci/5222,CERT-Polska-bedzie-wspoltworzyl-baze-podatnosci-CVE.html>



Zródło <https://www.nask.pl/pl/aktualnosci/5222,CERT-Polska-bedzie-wspoltworzyl-baze-podatnosci-CVE.html>



Apple aktywnie zwalcza cyberzagrożenia w swoich produktach

W połowie lipca br. firma *Apple* na portalu *support.apple.com* upubliczniła zestaw aktualizacji oprogramowania dla wytwarzanych przez siebie produktów. Pakiet zabezpieczeń eliminuje wykryte podatności typu *zero-day*. *Apple* w wystosowanym komunikacie stwierdza, że luka oznaczona jako CVE-2023-37450 mogła być aktywnie wykorzystywana przez cyberprzestępców w atakach na urządzenia typu m.in. *iPhone*, *Macbook* oraz *iPad*. Podatność znajdowała się w open-source'owym silniku przeglądarek internetowych o nazwie *WebKit*. Wyżej wymienione narzędzie stosowane jest m.in. w aplikacjach *Safari*, *AppStore*, *Mail* oraz wielu innych programach używanych w systemach operacyjnych *IOS* oraz *Linux*. Aktywne użycie luki umożliwiało przeprowadzenie atak typu *zdalne wykonanie kodu* (ang. *Remote Code Execution*).

Pośród ostatniej paczki aktualizacji znalazły się również rozwiązania niwelujące krytyczne podatności oznaczone numerami:

- CVE-2023-38606,
- CVE-2023-32434,
- CVE-2023-32435,
- CVE-2023-32439.

Ponadto zespół bezpieczeństwa *Apple* zмага się z systematycznymi atakami polegającymi na podszywaniu się złośliwych aplikacji pod prawdziwe rozwiązania legalnych dostawców. Na liście

najpopularniejszych produktów w sklepie *AppStore* w Europie znalazła się aplikacja *Threads*, która podszywała się pod rozwiązanie firmy *Meta*. Jednakże ze względu na konieczność dostosowania oprogramowania do europejskiego prawa w zakresie prywatności użytkowników, concern Marka Zuckerberga nie wydał jeszcze oficjalnej, dedykowanej, europejskiej dystrybucji aplikacji dla swojego najnowszego portalu internetowego.

SocialKit LTD tworząc swoją fałszywkę wzorowali się na rozwiązaniu dostarczonym przez *Meta* na rynki azjatyckie. Konto ww. dostawcy zostało już zablokowane przez sklep *AppStore*. Pośród innych złośliwych aplikacji oferowanych przez *SocialKit LTD* znajdowały się: *ChatGP*, *SelfMe*, *Selfie AI Face Editor*, and *Remove Background Eraser*.

Rekomendacje: celem uniknięcia wykorzystania krytycznych podatności przez cyberprzestępców do przejścia wrażliwych danych z Twojego urządzenia firmy *Apple*, jak najszybciej zaktualizuj swoją wersję oprogramowania. Link z informacjami dot. aktualizacji: <https://support.apple.com/en-us/HT213823>. Ponadto sprawdź czy na swoim urządzeniu nie posiadasz aplikacji od firmy *SocialKit LTD* – jeżeli tak, natychmiast je usuń.

Źródła: *BleepingComputer.pl*, *HackRead.com*, *WebKit.org*, *Apple.com*



Logo firmy Apple

Źródło: <https://www.bleepingcomputer.com/news/apple/apple-fixes-new-zero-day-used-in-attacks-against-iphones-macs/>



WormGPT - AI w rękach cyberprzestępców

Skokowy rozwój generatywnej sztucznej inteligencji oraz udostępnienie szerokiego wstępu użytkownikom Internetu do dużych modeli AI jak *ChatGPT* i *OpenAI*, zmienia nie tylko życie zwykłych Internautów, ale wpływa również na czarny rynek cyberbezpieczeństwa oraz przestępców z niego korzystających. *WormGPT* – zwany *Chat'emGPT* dla hakerów, jest to narzędzie stworzone przy wykorzystaniu dużego modelu językowego AI, służące do pisania złośliwego kodu i innego typu *malware*. Ww. oprogramowanie umożliwia tworzenie efektywnych złośliwych rozwiązań w wyjątkowo prosty i tani sposób (dostęp zaczyna się od niespełna 46 Euro miesięcznie).



WormGPT poza możliwością automatycznego pisania złośliwego oprogramowania w języku *Python*, dostarcza wskazówki dot. strategii użycia oraz informacji nt. rozwiązania problemów związanych z obsługą wytworzonego *malware'u*. Rozwiązanie oparte jest na specjalnie przygotowanym modelu językowym wydanym w 2021 r., o nazwie *GPT-J*.

Autor bloga *Slashnext*² (link w Źródłach) opisuje możliwość wykorzystania ww. rozwiązania do wsparcia akcji phishingowych prowadzonych w atakach typu *Business Email Compromise* (BEC). *Slashnext* przy użyciu *WormGPT* tworzy wiadomości praktycznie niemożliwe do odróżnienia od prawdziwych maili biznesowych. Jakość generowanych treści poprawnością stosowanego języka przewyższa wielu jego naturalnych użytkowników.

Rekomendacje: celem ataków typu BEC 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*). Ponadto w przypadku otrzymania wiadomości z poza organizacji, o treści wskazujących na potrzebę przekazania danych wrażliwych, logowania lub dokonania przelewów finansowych, zalecamy potwierdzenie procedury alternatywnym kanałem kontaktowym.

Źródła: *SlashNext.com*, *IThardware.pl*

² <https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/eu>



Kampanie przestępcze w lipcu 2023 oczami CSIRT KNF

Wakacje w pełni, nie jest to jednak czas odpoczynku od działań podejmowanych przez cyberprzestępców, a wręcz przeciwnie! Niejednokrotnie wakacje, urlopy, wyjazdy, czas wolny to motywy jakimi oszuści posługują się w swoich działaniach socjotechnicznych. Tym razem nie było inaczej, podejmowali oni liczne działania celem wykradania danych uwierzytliwiających do bankowości elektronicznej, informacji o kartach płatniczych oraz danych osobowych. Tylko w lipcu 2023 roku, dzięki podjętym działaniom CSIRT KNF zgłosił do zablokowania 1 725 domen (dla porównania CERT Polska dodał na listę ostrzeżeń 4 693 domen). Obecnie na liście ostrzeżeń przed niebezpiecznymi stronami (CERT HOLE) znajduje się 129 678 domen.

Pierwszą część artykułu poświęcimy na te kampanie, które trwają już od długiego czasu, niestety nadal są skuteczną bronią w rękach cyberprzestępców. Mowa tu m.in. o kampanii, w której ofiarami oszustwa padają osoby wystawiające przedmiot lub usługę na portalach ogłoszeniowych. Pod pretekstem zakupu wystawianego towaru wysyłany jest do nich link, pod którym znajduje się strona phishingowa. Kolejnym znanym schematem są fałszywe sklepy, które kuszą konkurencyjnymi cenami, a w rzeczywistości wyłudniają pieniądze. Kolejnym, niezmiennym przykładem są podszycia pod platformę streamingową *Netflix* i informowanie o rzekomym zawieszeniu konta. W lipcu 2023 te kampanie były dystrybuowane zarówno poprzez wiadomości SMS, jak i e-mail. Dodatkowo przestępcy podszywali się także pod platformy *Disney+* oraz *Amazon Prime*. Podobnie niezmiennie istotny wyzwaniem jest schemat znany pod nazwą „fraud inwestycyjny”, czyli sytuacja, w której osoba oszukiwana daje się namówić na rzekomą możliwość pewnego zysku. A następnie oszuści przy wykorzystaniu licznych metod manipulacyjnych nakłaniają ofiarę do wpłacania wysokich kwot pieniężnych. Najczęściej jest tak, że dopiero w momencie kiedy ofiara chce wypłacić obiecane środki orientuje się, że jest oszukiwana. Jednak w lipcu 2023 analizowaliśmy wprowadzenie nowego elementu do opisywanego schematu. Tym razem, mając nadal kontrolę nad zmanipulowaną osobą, gdy ta twierdzi, że koniecznie chce wypłacić rzekomo zarobione pieniądze, przestępcy zgadzają się, jednocześnie twierdząc, że w ramach formalności musi ona „sprawdzić swoje konto bankowe za pomocą systemu AML”.

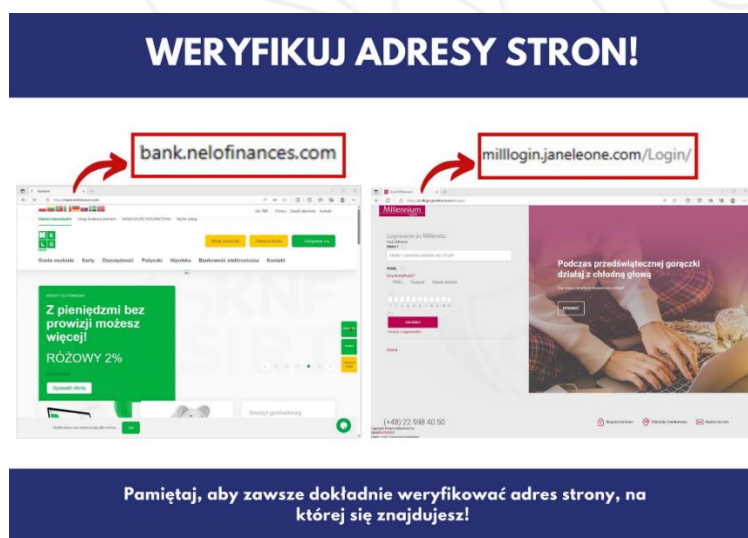
Strona, do której przysyłają link, wykorzystywała wizerunek Komisji Nadzoru Finansowego, aby zwiększyć wiarygodność prowadzonego scenariusza. Następnie poszkodowany przekierowywany był do strony łudząco przypominającej bankowość internetową swojego banku. To tutaj, pod pretekstem potrzeby zalogowania się i dokończenia weryfikacji oszuści starali się przechwycić dane. A jakby tego było jeszcze mało, to postanowili spróbować oszukać osoby, które już raz dały się nabrać. Podszywając się pod Interpol oraz powołując na rzekomy news w *BCC NEWS* ogłosili o rzekomym aresztowaniu osób wyłudających pieniądze i możliwości ich odzyskania. Po wejściu w link z reklamy, ofiara trafiała na stronę, na której musiała wpisać swoje dane osobowe oraz podać informację na jaką kwotę została oszukana. W kolejnym etapie na podane dane przestępcy wykonywali połączenie głosowe. Tym sposobem starali się wyłudzić kolejne, wysokie kwoty pieniędzy.

Z bardziej wakacyjnych motywów kampanii przestępczych, analizowaliśmy podszycie się pod stacje benzynowe i informacje o rzekomej możliwości zdobycia kuponów paliwowych. A także



wykorzystanie wizerunku polskiego przewoźnika kolejowego – *PKP Intercity* i ogłoszenie o kuponach na darmowe przejazdy. W ten sposób przestępcy wyłudzali poświadczenia logowania oraz dane kart płatniczych. W lipcu 2023 roku miały również miejsce kampanie podszywające się pod polskie banki. Dla przykładu, przestępcy wykorzystując markę *Millennium Bank* oraz *BNP Paribas* (rys. 1) wystawiali reklamy w mediach społecznościowych informujące, czy to o możliwości zdobycia pieniędzy, czy udziału w loterii z nagrodami, w rzeczywistości wyłudzając dane.

Z kolei podszywając się pod *Velo Bank* (rys. 1) wykupili reklamę w wyszukiwarce Google. Następnie pod pretekstem udzielania rzekomych pożyczek windykacyjnych (dla osób bez zdolności kredytowych), zachęcali do wejścia na stronę phishingową. Po kliknięciu w link ofiara trafiała na formularz, który należało wypełnić danymi osobowymi, a następnie na stronę imitującą bankowość internetową. Po wypełnieniu danych, przekazywane były one do przestępców.



Przykład fałszywych stron podszywających się pod banki

W ramach prowadzonych analiz Cyber Threat Intelligence, *CSIRT KNF* w lipcu 2023 roku przygotował 3 raporty publiczne dotyczące działań przestępców. Są to:

- międzynarodowa kampania phishingowa - opisującym globalną kampanię phishingową, w której przestępcy podszywali się pod instytucje pocztowe na całym świecie - w tym naszą rodzimą, Poczta Polska; link: https://cebrf.knf.gov.pl/images/Midzynarodowa_Kampania_Phishingowa_PL-2_1.pdf
- analiza malware z Youtube - analiza złośliwego oprogramowania znalezionej na platformie YouTube. Skupia się na konkretnym przypadku, w którym został użyty link do pobrania z opisu filmu, reklamującego oprogramowanie typu crack do popularnej aplikacji *Acrobat Reader*. Po pobraniu i analizie zawartości pliku .rar, stwierdzono, że zawiera on złośliwe oprogramowanie skupiające się na kradzieży informacji z urządzenia ofiary; link: https://cebrf.knf.gov.pl/images/Malware_Youtube_PL.pdf



- wykorzystanie technologii *WebAPK* do ataku phishingowego - analiza wyrafinowanego ataku phishingowego, który wykorzystywał technologię *WebAPK* do instalacji szkodliwej aplikacji na urządzeniach z systemem Android, wykrytego w analizie kampanii phishingowej podszywającej się pod *PKO BP*; link: <https://cebrf.knf.gov.pl/komunikaty/artykuly-csirt-knf/362-ostrzezenia/874-wykorzystanie-tehnologii-webapk-do-ataku-phishingowego>

Jak widać, atakujący nie próżnują, kontynuując znane, ale niestety nadal skuteczne scenariusze kampanii phishingowych, jak i wymyślając nowe sposoby na wyłudzenie czy to wrażliwych danych, czy bezpośrednio środków pieniężnych. *CSIRT KNF* na bieżąco śledzi i analizuje nowe sposoby działania oszustów, o których informuje za pośrednictwem mediów społecznościowych: [Twitter](#), [LinkedIn](#) oraz [Facebook](#). Natomiast ze szczegółami kampanii przestępczych obserwowanych zarówno w lipcu 2023, jak i poprzednich miesiącach zapoznać się można na naszej stronie: <https://cebrf.knf.gov.pl/komunikaty/artykuly-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: <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 konsultentów) 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 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: <https://cert.pl/tlp/>