Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

09/2023

Wieloletnia operacja szpiegowska chińskiej grupy APT *TAG-74* 3

USA przygotowują się na erę post-kwantową 4

Rosyjskie cyberataki na Ukrainę 5

Bieżący rok może okazać się rekordowy pod względem upublicznionych podatności typu *zero-day* przy spadku ogólnej liczby luk bezpieczeństwa 6

Stany Zjednoczone tworzą jeden krajowy podmiot agregujący zgłaszane incydenty cybernetyczne oraz koordynujący ich dystrybucję do właściwych organów 7

Polska znalazła się na 6. miejscu w rankingu cyberbezpieczeństwa oraz bierze udział w 11. edycji *Europejskiego Miesiąca Cyberbezpieczeństwa* 8

Ukraińskie wojsko celem kampanii phishingowej *STARK#VORTEX* wykorzystującej instrukcje obsługi dronów 9

Nowe techniki ataków phishingowych: *ZeroFont*, reklamy w *Bing Chat* oraz *DarkGate* malware w *MS Teams* 10

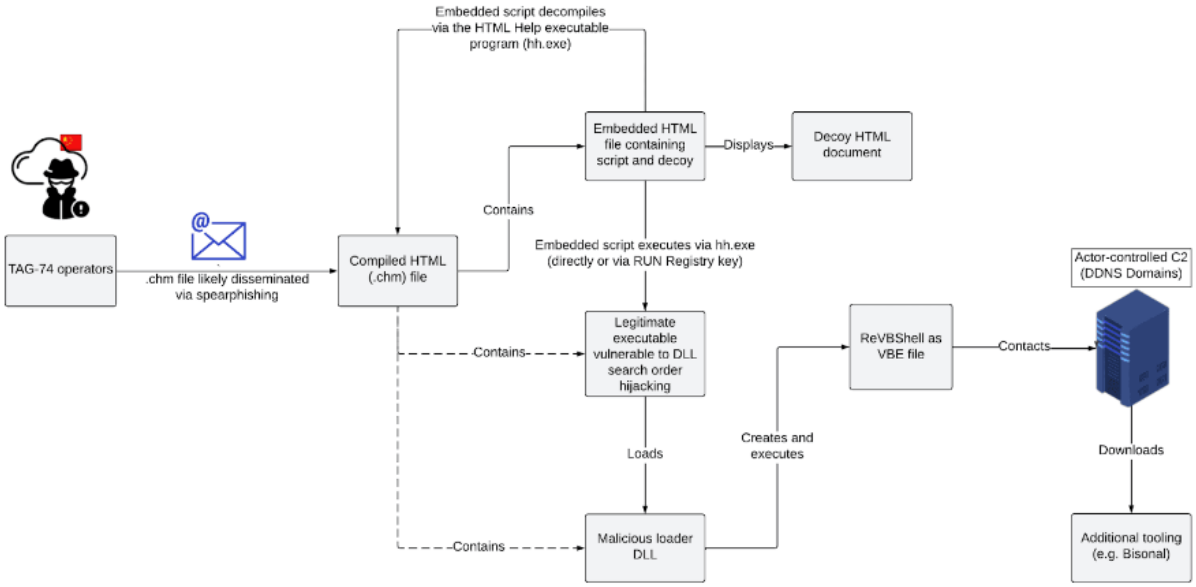
Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta 11

INFORMACJA O SZKOLENIACH 13

Oznaczenia TLP 14

Wieloletnia operacja szpiegowska chińskiej grupy APT *TAG-74*

Badacze bezpieczeństwa z *Insikt Group* z *Recorded Future* udostępnili analizę długookresowej kampanii o charakterze szpiegowskim w cyberprzestrzeni. Odpowiedzialność za ataki została przypisana chińskiej grupie APT – *TAG-74*, przypisywanej przez specjalistów do wywiadu wojskowego Państwa Środka (*state sponsored*). Wg analiz, działalność *TAG-74* skoncentrowana jest przede wszystkim na infiltracji południowokoreańskich organizacji akademickich, politycznych oraz rządowych. Ponadto przyjmuje się, że stanowi ona poważne zagrożenie dla podmiotów z obszarów technologii lotniczych, obronnych i wojskowych nie tylko w Korei Południowej, ale także w Japonii oraz Rosji. Ataki *TAG-74* na instytucje z ww. obszarów są zgodne ze stosowaną przez Pekin polityką polegającą na wsparciu działań w cyberprzestrzeni, prowadzonych celem szpiegostwa przemysłowego oraz kradzieży własności intelektualnej z zakresu nowych technologii i z obszarów wrażliwych.



Schemat ataku. Źródło: recordedfuture.com

Upubliczniony atak oparty był na dystrybuowaniu przez grupę spreparowanych wiadomości mailowych (*phishing*) zawierających pliki *MS Compiled HTML Help* (CHM), przekazywanych z zamiarem dostarczenia wariantu *backdoora Visual Basic Script* o nazwie *ReVBShell*. Uruchamiał on trojana *Bisona* (jest to wielofunkcyjny trojan, posiadający zdolności: agregacji informacji o procesach i plikach, wykonywania poleceń kodu i tworzenia plików, zamykania procesów, pobierania i transferu danych oraz kasowania dowolnych plików na zainfekowanym dysku*)*. Konfiguracja *ReVBShell* powodowała uśpienie trojana przez zdefiniowany czas. Ruch między implantem a C2 maskowany był kodowaniem *Base64*.

Sposób wykorzystania *ReVBShell* został wcześniej powiązany z dwoma innymi chińskimi grupami hakerskimi *Tick* (*RedBaldKnight*) i *Tonto Team* (m.in. *Earth Akhlut*). W kwietniu br. identyczna sekwencja infekcji została wykryta przez *AhnLab Security Emergency Response Center* (ASEC).

Źródła: recordedfuture.com, thehackernews.com, attack.mitre.com

USA przygotowują się na erę post-kwantową

Technologie kwantowe zaliczane są do przełomowych, tj. takich, które będą miały radykalny wpływ na wszystkie obszary funkcjonowania społeczeństwa, gospodarki i państwa, także w obszarze bezpieczeństwa i obronności. Jednym ze skutków zastosowania odpowiednio zaawansowanych komputerów kwantowych będzie możliwość szybkiego rozszyfrowania informacji zabezpieczonych dotychczas stosowanymi metodami kryptograficznymi.

Szereg państw podjął działania, aby przygotować się na rewolucję kwantową i zawczasu opracować rozwiązania, które pozwolą zachować poufność danych, uniemożliwić proste złamanie dotychczasowych algorytmów kryptograficznych.

W maju 2022 r. prezydent USA wydał Memorandum dotyczące bezpieczeństwa narodowego w kwestii promowania przywództwa Stanów Zjednoczonych w dziedzinie obliczeń kwantowych przy jednoczesnym ograniczaniu ryzyka dla wrażliwych systemów kryptograficznych. Dokument ten nie tylko określa kierunki, które mają zagwarantować USA przewagę w technologiach kwantowych, ale także kieruje konkretne zadania dla poszczególnych agend rządowych z konkretnymi terminami, które powinny zrealizować, aby zabezpieczyć proces migracji systemów komputerowych do kryptografii postkwantowej. W ramach tych działań *Narodowy Instytut Standardów i Technologii* (NIST) oraz *Agencja Bezpieczeństwa Narodowego* (NSA) do 2024 r. mają opracować standardy techniczne dla kryptografii kwantowoodpornej.

W nawiązaniu do tego procesu *Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury* (CISA) wraz z NIST i NSA wydały opracowanie o migracji do postkwantowej kryptografii, w którym opisują wyzwania związane z rewolucją kwantową oraz zachęcają do zaplanowania migracji do postkwantowych standardów kryptograficznych. Warto zapoznać się z działaniami, które należy podjąć, aby zachować bezpieczeństwo informacji w swojej organizacji, gdy technologie kwantowe osiągną odpowiednią dojrzałość.

Źródło: CISA

Rzeczywistość postkwantowa jest także wyzwaniem dla Polski, zarówno pod kątem posiadania rodzimych rozwiązań kryptograficznych (zob. np. projekty *OptoKrypt*, *PIONIER-Q*, czy wyżarzania kwantowego), jak i opracowania odpowiednich standardów kryptograficznych, zarówno dla cyfrowych usług komercyjnych i publicznych, jak i informacji niejawnych.

Źródła: CISA, White House.

Rosyjskie cyberataki na Ukrainę

Ukraińska Państwowa Służba Łączności Specjalnej i Ochrony Informacji przedstawiała raport nt. rosyjskich cyberataków w 2022 i I połowie 2023 r. Służba, w której funkcjonuje CERT UA, informuje, że jednym z głównych celów ataków o charakterze cyberszpiegowskim były organy ścigania, co wiązało się z próbami przejęcia dowodów rosyjskich zbrodni wojennych oraz danych osób podejrzanych o szpiegostwo na rzecz Rosji. Podkreśla się też, że sponsorowani przez państwo hakerzy biorą na cel te same ofiary, aby pozyskać krytyczne dane dla działań rosyjskiej armii. Raz zinfiltrowane organizacje dostarczają wiedzy infrastruktury sieciowej, środków bezpieczeństwa, czy kluczowego personelu.

W kwestiach technicznych warto zwrócić uwagę na skoncentrowaniu na natychmiastowej ekstrakcji danych. Wynika to z tego, że CERT UA i jego partnerzy optymalizują gromadzenie informacji o zagrożeniach (TI) oraz skrócili średni czas wykrycia i reakcji. Spowodowało to, że rosyjscy hakerzy po włamaniu się do systemu chcą najszybciej pozyskać cenne dane, następnie rozpoczynają rozpowszechnianie złośliwego oprogramowania różnymi kanałami do innych ważnych celów, korzystając z zaufania do zinfiltrowanego użytkownika.

Rośnie również wykorzystanie metod "*Living Off The Land*". Intruzi wykorzystują wbudowane funkcjonalności systemu lub zewnętrzne narzędzia do wykonywania złośliwych działań w systemie (np. *WinRar* i narzędzia Windows). Utrudnia to wykrycie działań przez systemy antywirusowe i EDR.

Ukraińska Służba jako główne sektory będące calami cyberataków wskazuje energetykę i media. W kwestii tego pierwszego kluczowym problemem prowadzącym do skutecznej penetracji jest brak odpowiedniej izolacji pomiędzy systemami OT a sieciami korporacyjnymi.

Źródło: SSSCIP

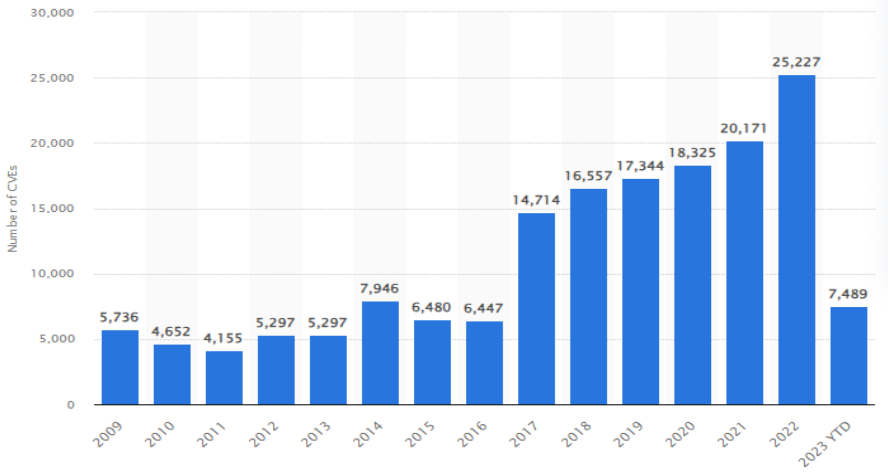
Polska również pozostaje jednym z głównych celów rosyjskich cyberataków, co pokazuje m.in. ostatni raport *Microsoftu*, a więc nasz kraj musi ciągle zwiększać swoją odporność na zagrożenia w cyberprzestrzeni, w tym te, za którymi stoją grupy sponsorowane przez wrogie nam państwa. W odniesieniu do kwestii natychmiastowej ekstrakcji danych warto odpowiednio zwiększać zdolności w zakresie *Threat Intelligence* oraz automatyzacji i autonomiczności systemów zabezpieczeń. Natomiast w zakresie stosowania metody "*Living Off The Land*" istotne jest wdrożenie szeregu rozwiązań w organizacji, które pozwolą zminimalizować to zagrożenie, związanych m.in. z architekturą bezpieczeństwa, wydzieleniem systemów, audytami, zwróceniem szczególne uwagi na podejrzane załączniki, wymuszeniem używania podwójnego uwierzytelniania. Warto też zwrócić uwagę na materiał CISA poświęcony chińskiej kampanii przy wykorzystaniu tej metody.

Źródła: SSSCIP, Microsoft, CISA.

Bieżący rok może okazać się rekordowy pod względem upublicznionych podatności typu *zero-day* przy spadku ogólnej liczby luk bezpieczeństwa

Firma *Mandiant* informuje, że przez pierwsze dziewięć miesięcy bieżącego roku światowi badacze oraz zespoły bezpieczeństwa opublikowali 70 krytycznych podatności typu zero-day, które zostały dodane do biblioteki CVE. Dla porównania należy zaznaczyć, że w całym 2022 r. wykryto ich 55, a w rekordowym 2021 r. – 81. Z 70 zero-day'ami odkrytymi do tej pory 2023 r. jest na prostej drodze do ustanowienia nowego rekordu. Wrzesień z 10 opublikowanymi lukami okazał się wyjątkowo efektywny w stosunku do miesięcy poprzednich w których upubliczniono ich łącznie 60.

Według portalu *statista.com* liczba wszystkich zarejestrowanych podatności do końca sierpnia br. wyniosła blisko 7,5 tys. Prognozowana na podstawie średniej miesięcznej liczba luk na koniec 2023 r. wyniesie 12 tys. co stanowi wyraźny spadek r/r, w stosunku do blisko 25,3 tys. w całym 2022 r.



Wykres liczby opublikowanych podatności na przestrzeni lat. Źródło: statista.com

Specjaliści od rynku IT stwierdzają, że zmiany w ilości wykrywanych i udostępnianych podatności wynikają z po pandemicznych zmian w strukturze zatrudnienia przedsiębiorstw. Nagła potrzeba wzrostu zatrudnienia w IT; rynkowa konkurencja w ilości i jakości dostępnych usług cyfrowych; automatyzacja procesów testowania rozwiązań; wzrost popularności usług chmurowych; większy nacisk na zespoły cyberbezpieczeństwa; outsourcing usług programistycznych; rosnąca świadomość potrzeby inwestowania środków finansowych w cyberbezpieczeństwo przez kadry kierownicze – spowodowały wzrost bezpieczeństwa wydawanych produktów i rozwiązań końcowych, co za tym idzie spadek występowania luk bezpieczeństwa oraz wzrost koncentracji na wciąż stosunkowo bardzo rzadkich podatnościach typu *zero-day*.

Rekomendacje: utrzymanie bezpieczeństwa systemów IT wymaga stałej aktualizacji oprogramowania do najnowszych wersji udostępnianych przez producenta. Dostawca zwyczajowo implementuje najnowsze łatki dla upublicznionych podatności. Niezałatane luki mogą skutkować incydentami krytycznymi o wysokich konsekwencjach prawnych lub finansowych jak np. wyciek danych (data leak) lub zaszyfrowaniem danych (ransomware).

Źródła: *statista.com, cve.mitre.org, arstechnica.com*

Stany Zjednoczone tworzą jeden krajowy podmiot agregujący zgłaszane incydenty cybernetyczne oraz koordynujący ich dystrybucję do właściwych organów

Niezaprzeczalnym jest, że świat cyfrowy stał się integralną częścią świata rzeczywistego. Dlatego też ze względu na swoją skalę i złożoność wypływające z niego zagrożenia stanowią ryzyko powstawania szkód zarówno dla życia ludzkiego (np. przerwy w dostawach energii czy leków), jak i majątków ludzkich (np. ataki ransomware, data leaks). Niepodważalnym jest również fakt, że wraz z rosnącym poziomem cyfryzacji gospodarki i społeczeństwa wzrasta liczba ataków cybernetycznych.

W reakcji na ilość, skale i poziom zaawansowania technicznego zagrożeń rośnie również liczba specjalistycznych podmiotów odpowiedzialnych za udzielnie wsparcia w reakcji na nie.

Okładka raportu DHS. Źródło dhs.gov

W sytuacji ataku na osoby czy przedsiębiorstwa, ofiary są zobligowane do niezwłocznego poinformowania o zdarzeniu właściwe organy. Skomplikowanie ataków czy wielobranżowość prowadzonej działalności przez ofiary sprawia, że niektóre z nadużyć są trudne do zdefiniowania, co znacznie komplikuje wskazanie konkretnej instytucji odpowiedzialnej za przyjęcie zgłoszenia i ewentualne udzielenie wsparcia. Złożoność procedur jest czynnikiem hamulcowym dla podjęcia szybkiej, często kluczowej reakcji zarówno dla zaatakowanego podmiotu (absorbując jego czas oraz zasoby techniczne i ludzkie), jak i przez instytucje publiczne zobligowane do obsługi incydentu (ze względu na procedury formalne uniemożliwiające podjęcie reakcji), przy czym każda kolejna minuta może zwiększać powodowane straty. Dlatego też, cyfryzacja powinna mieść swój własny… Krajowy System Ratowniczo-Gaśniczy, gdzie jest jeden punkt kontaktowy jak Centrum Powiadamiania Ratunkowego przyjmujący zgłoszenia (numer 112), a następnie deleguje odpowiednie instytucje czyli… CSIRTy.

Z zamiarem rozwiązania powyższego problemu Departament Bezpieczeństwa Wewnętrznego (DHS) US przedstawił koncepcję pojedynczego portalu internetowego do zgłaszania większości krajowych incydentów cybernetycznych. Portal skierowany jest dla krajowych podmiotów będących ofiarami takich ataków. Rozwiązanie ma na celu uproszczenie zasad zgłaszania incydentów cybernetycznych oraz przyśpieszenie procedury umożliwiającej reakcję i wparcie dedykowanych organów.

W ramach projektu CISA otrzymała zadanie usprawnienia obowiązujących przepisów dot. obecnie 52. różnych portali agregujących zgłoszenia. Zawierały one nieustandaryzowane formularze oraz wymagały od ofiar informacji różnego rodzaju, często się powtarzających. W ramach jednego portalu i zunifikowanego formularza będzie można zgłosić incydent do m.in. do: *DHS, Departamentu Skarbu, Obrony, Sprawiedliwości, Rolnictwa i Handlu, Komisji Papierów Wartościowych i Giełd, Federalnej Komisji Handlu i Federalna Komisja Łączności* oraz kilkudziesięciu innych instytucji.

Źródła: therecord.com, dhs.gov

Polska znalazła się na 6. miejscu w rankingu cyberbezpieczeństwa oraz bierze udział w 11. edycji *Europejskiego Miesiąca Cyberbezpieczeństwa*

The Cyber Defense Index 2022/23 opublikowanym przez magazyn *MIT Technology Review* - to globalne zestawienie 20 największych gospodarek świata (z wyłączeniem Rosji), w którym oceniane jest m.in., w jakim stopniu poszczególne państwa wdrożyły praktyki zapobiegania cyberatakom i na ile lokalne regulacje wspierają działania w tym zakresie. Dane pochodzą z zasobów instytucji międzynarodowych i globalnej ankiety przeprowadzonej wśród kadry kierowniczej odpowiedzialnej za cyberbezpieczeństwo w swoich organizacjach. W ocenie uwzględnione zostały cztery aspekty: infrastruktura krytyczna, zasoby cyberbezpieczeństwa, zdolności organizacyjne oraz regulacje i otoczenie prawne. Polska otrzymała w tym rankingu całościową ocenę 6,91, przy czym najwyżej oceniono jej zasoby cyberbezpieczeństwa – na 7,34 punktu. Najlepszym wynikiem pochwalić może się Australia, której *The Cyber Defense Index 2022/23* oceniany jest na 7,83 punktu.

Polska nie spoczywając na laurach rozwija świadomość cyfrową obywateli biorąc udział w kolejnej, **11 edycja *Europejskiego Miesiąca Cyberbezpieczeństwa* (ECSM**). Jest to kampania organizowana przez *Agencję Unii Europejskiej ds. Cyberbezpieczeństwa* (ENISA) z inicjatywy *Komisji Europejskiej*. ECSM nawiązuje ona do amerykańskiego *Dnia Świadomości Cyberbezpieczeństwa* organizowanego przez CISA, który odbywa w październiku już od 20 lat.

Badacze zgodnie stwierdzają, że najsłabszym ogniwem i najpoważniejszą luką bezpieczeństwa jest człowiek. Dlatego też. obecne działania skupiają się na promocji cyberbezpieczeństwa i wiedzy nt. zagrożeń w sieci celem budowy świadomości zagrożeń (eng. *awareness*). Tematem przewodnim tegorocznej edycji są zagrożenia skupione wokół socjotechniki w sieci (*scam*, *phishing*, *vishing*, *smishing* itp.). Kampania ECSM polega na zgłaszaniu przez firmy i inne instytucje inicjatyw z zakresu cyberbezpieczeństwa, celem podnoszenia świadomości i kompetencji w tym zakresie. Kampania ma charakter niekomercyjny, a udział w inicjatywach jest bezpłatny. Przykładami inicjatyw są m.in. webinary czy konferencje.

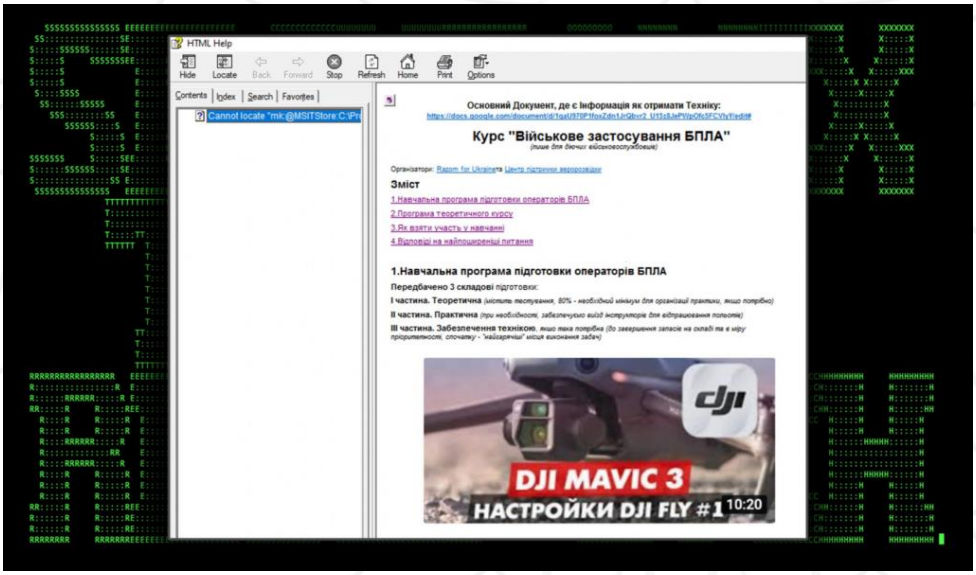
Zapraszamy do wzięcia udziału w tegorocznej edycji kampanii ECSM i zgłaszania swoich inicjatyw poprzez **formularz** na stronie oraz śledzenie aktualności na profilach ECSM w mediach społecznościowych: *FB:* ***https://www.facebook.com/ECSMPL*** i *Twitter(X):* ***https://twitter.com/ecsmpolska.*** Wszystkie materiały związane z tegoroczną edycją kampanii ECSM a także zgłoszone inicjatywy będą na bieżąco publikowane na stronie internetowej ***https://bezpiecznymiesiac.pl/***.

Źródła: cisa.gov, nask.pl, enisa.europa.eu, cbzc.policja.gov.pl, nask.pl, cyberdefence24.pl

Ukraińskie wojsko celem kampanii phishingowej *STARK#VORTEX* wykorzystującej instrukcje obsługi dronów

Według raportu *Securonix* z 25 września 2023 r. wykryto kampanię phishingową o nazwie *STARK#VORTEX*, przypisywaną grupie hakerskiej "*UAC-0154*", której celem były ukraińskie organizacje wojskowe. Kampania ta wykorzystywała fałszywy plik instrukcji obsługi drona *Pilot-in-Command* (PIC) do dystrybucji oprogramowania typu *stealware* o nazwie *MerlinAgent*. *MerlinAgent* jest znany ze swojej zdolności do skrytego wykradania danych i ukrytych technik infiltracji.

Grupa hakerska rozprzestrzeniała złośliwy plik *Microsoft Compiled HTML Help (.chm)* o nazwie "*І нфо про навчання по БПЛА для ві йськових.v2.2.chm*" w tłumaczeniu jako "*Informacje o szkoleniu wojskowym w zakresie bezzałogowych statków powietrznych*", który miał za zadanie skłonić ukraińską armię (odbiorców pliku) do uwierzenia, że jest to legalny plik instrukcji obsługi drona. Punktem wyjścia ataku jest ww. plik *.chm*, który po otwarciu uruchamia złośliwy kod *JavaScript* osadzony wewnątrz jednej ze stron *HTML* w celu wykonania kodu *PowerShell* zaprojektowanego do kontaktowania się ze zdalnym serwerem w celu pobrania zaciemnionego pliku binarnego. Ładunek oparty na systemie *Windows* jest dekodowany w celu wyodrębnienia agenta *Merlin*, który z kolei jest skonfigurowany do komunikacji z serwerem dowodzenia i kontroli (C2) w celu podjęcia działań po eksploitacji, skutecznie przejmując kontrolę nad hostem. Chociaż łańcuch ataku jest dość prosty, atakujący wykorzystali dość złożone TTP i metody zaciemniania, aby uniknąć wykrycia.



Plik, który otrzymywały ofiary ataku, jako instrukcja obsługi drona. Źródło: securonix.com

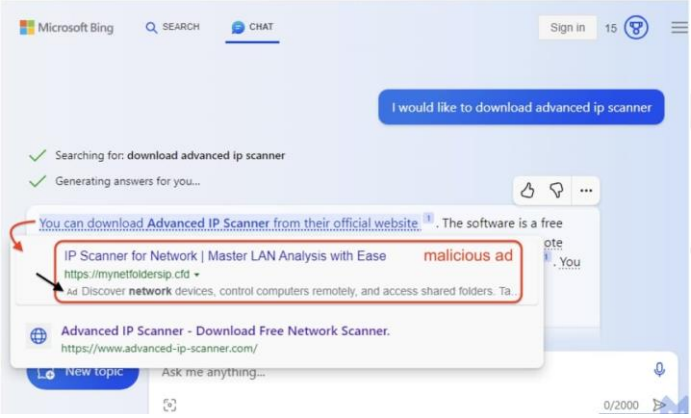
Rekomendacje: Odkąd drony lub bezzałogowe statki powietrzne (UAV) stały się integralnym narzędziem wykorzystywanym przez ukraińskie wojsko, zaczęły pojawiać się pliki-przynęty zawierające złośliwe oprogramowanie, udające instrukcje obsługi UAV. Z uwagi na popularność tego typu sprzętów, należy uważać skąd pobieramy pliki związane z ich obsługą i konfiguracją, również jako polscy użytkownicy, mogący stanowić potencjalny cel podobnego ataku hakerskiego.

Źródła: *thehackernews.com, securonix.com*

Nowe techniki ataków phishingowych: *ZeroFont*, reklamy w *Bing Chat* oraz *DarkGate* malware w *MS Teams*

Jedną z ostatnich kampanii jest phishing *ZeroFont*, w której cyberprzestępcy ustawiają rozmiar czcionki słów lub znaków w wiadomościach e-mail na zero, dzięki czemu tekst jest niewidoczny dla ludzi, podczas gdy systemy przetwarzania języka naturalnego (NLP) mogą go nadal czytać. W ataku *ZeroFont* ukryty tekst jest używany do tworzenia fałszywej wiadomości skanowania bezpieczeństwa w okienku listy wiadomości e-mail w programie *Microsoft Outlook*. Odbywa się to poprzez wstawienie następującego kodu na początku treści wiadomości e-mail: *Isc Advanced Threat protection: This message has been scanned for threats.*. Ten tekst jest niewidoczny dla odbiorcy, ale jest wyświetlany w okienku listy wiadomości e-mail w programie *Outlook*, dzięki czemu wygląda na to, że wiadomość e-mail została przeskanowana pod kątem zagrożeń i można ją bezpiecznie otworzyć.

Hakerzy wykorzystują również reklamy online w odpowiedziach *Bing Chat* opartych na sztucznej inteligencji, promując fałszywe witryny do dystrybucji złośliwego oprogramowania. Złośliwe reklamy udawały w ostatnim czasie prawdziwe witryny pobierania popularnego narzędzia "*Advanced IP Scanner*". Gdy użytkownik zapytał *Bing Chat*, jak pobrać *Advanced IP Scanner*, wyświetliłby się link do pobrania go na czacie. Jednak po najechaniu kursorem na podkreślony link na czacie, *Bing Chat* może najpierw wyświetlić reklamę, a następnie legalny link do pobrania. W tym przypadku link sponsorowany był reklamą promującą złośliwe oprogramowanie.



Złośliwy adres URL, który otrzymał użytkownik w konwersacji z Bing Chat. Źródło: Malwarebytes

Należy również wspomnieć o nowej kampanii phishingowej wykorzystującej wiadomości *Microsoft Teams* do wysyłania załączników, które instalują złośliwe oprogramowanie *DarkGate*. Skompromitowane wcześniej konta zostały wykorzystane do nakłonienia innych użytkowników *Microsoft Teams* do pobrania i otwarcia pliku *.zip* o nazwie "*Zmiany w harmonogramie urlopów*". Kliknięcie załącznika powoduje pobranie pliku *.zip* z adresu *URL SharePoint* i zawiera plik *.LNK* podszywający się pod dokument *.PDF*. Tym sposobem złośliwe oprogramowanie trafia na komputer ofiary.

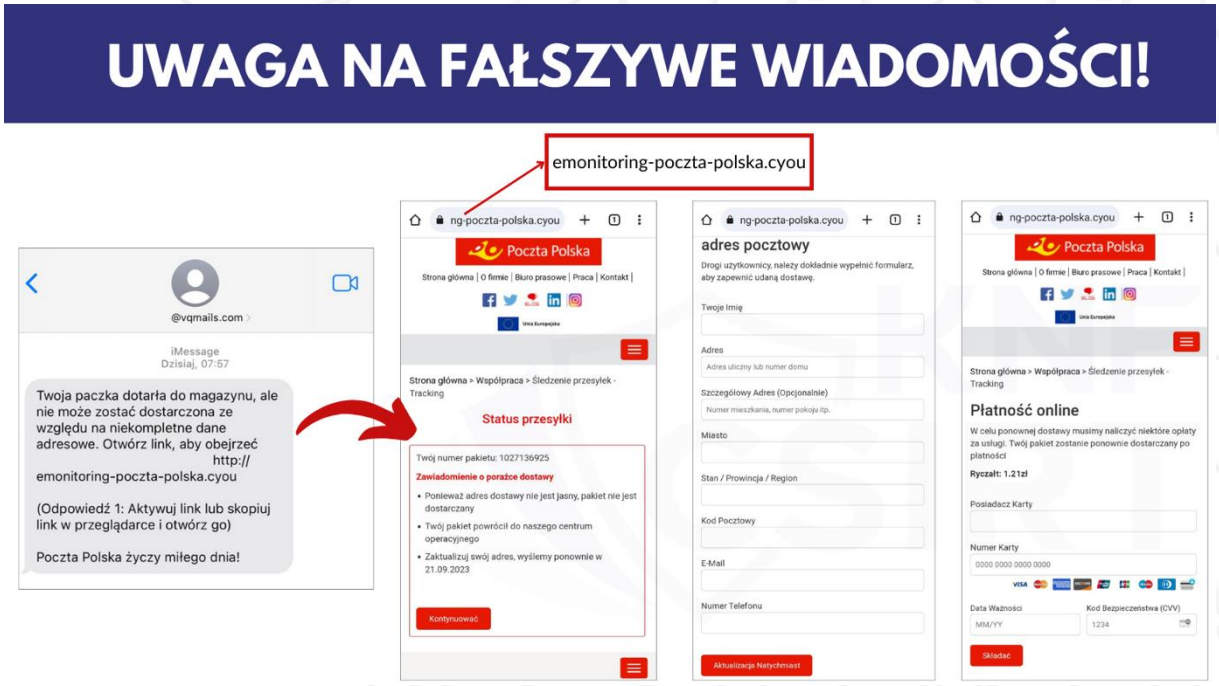
Rekomendacje: Zaleca się użytkownikom dokładne przeanalizowanie wiadomości e-mail przed otwarciem. Wyświetlanie złośliwych reklam w rozmowach na czacie Bing podkreśla rozszerzającą się granicę cyberzagrożeń i sprawia, że użytkownicy powinni uważać na wyniki chatbota i zawsze dokładnie sprawdzać adresy URL przed pobraniem czegokolwiek. Warto również skonfigurować Microsoft Teams tak, aby zezwalał na korespondencję tylko z określonymi podmiotami zewnętrznymi.

Źródła: bleepingcomputer.com, malwarebytes.com, medium.com

Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta

Wrzesień za nami, zatem pora na podsumowanie. W minionym miesiącu przez nasze ręce przeszło 4 521 domeny, które przeanalizowaliśmy i zgłosiliśmy do blokady. Za ich pomocą przestępcy próbowali pozyskać dane uwierzytelniające do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe (imię, nazwisko, adres zamieszkania, e-mail, numer telefonu etc.).

Cyberprzestępcy kilkukrotnie podszywali się pod polskie banki. Wykorzystując markę *BNP Paribas* rozesłali wiadomości e-mail, informując o blokadzie przelewu. Podszywając się pod ING rozesłali wiadomości SMS, informując o blokadzie karty. Jako *Credit Agricole* oszuści obiecywali pieniądze za wypełnienie ankiety, natomiast przedstawiając się jako *PKO BP* oferowali pożyczki. W obu ostatnich przypadkach fałszywe strony dystrybuowali poprzez wykupione reklamy na platformie *Facebook*. Czy to wszystko? Oczywiście, że nie! Cyberprzestępcy rozsyłali również SMS-y podszywające się pod strony rządowe (GOV) z informacją o niezapłaconej grzywnie za wykroczenie drogowe, czy o oczekującej na użytkownika wiadomości w portalu *mObywatel*. W innych, analizowanych przez nas przypadkach, przestępcy przedstawiali się jako *Binance* (giełda kryptowalut) oraz *UPS* (firma kurierska). We wrześniu 2023 r. cyberprzestępcy wykorzystali również funkcjonalność komunikatora internetowego opracowanego przez firmę *Apple* – *iMessage*. Rozesłali wiadomości SMS, w których nadawca przedstawiał się jako adres e-mail (rysunek). Podszywając się pod *Pocztę Polską* informowali o rzekomej potrzebie dostarczenia informacji o adresie, na który ma zostać dostarczona paczka. W rzeczywistości fałszywa strona wykradała dane karty płatniczej.



Przykłady ataków phishingowych

Kolejne przypadki miały miejsce na portalach społecznościowych, gdzie można było natrafić na fałszywe oferty sprzedaży produktu. Jak to zazwyczaj, w tego typu kampaniach phishingowych bywa, reklamowany towar można było rzekomo nabyć w konkurencyjnych cenach. W tym celu zostały wykorzystane marki sklepów *LIDL* oraz *Reserved*. Po wejściu na stronę, ofiara musiała wypełnić formularz osobowy, a następnie zachęcana była do wpisania danych karty płatniczej.

A na koniec, działanie przestępcze, które zdecydowanie zaskoczyło najbardziej... Znanych metod dystrybucji fałszywych domen jest wiele m.in. wiadomości SMS i e-mail, reklamy w *Google* oraz mediach społecznościowych, przejęte konta użytkownika, jednak cyberprzestępcy udowodnili, że *„o phishing można potknąć się nawet na ulicy"*. Za wycieraczkami wielu samochodów pojawiły się wydrukowane, fizyczne kartki z informacją o rzekomym otrzymaniu mandatu. Nadrukowany był na nich kod QR, który po zeskanowaniu prowadził do strony phishingowej, a ta wyłudzała dane kart płatniczych.

To co łączy te wszystkie kampanie phishingowe, to cel przestępczy. Starają się oni zachęcić ofiarę do wejścia w podanych (w wiadomości SMS, e-mail, reklamie w mediach społecznościowych, czy na kartce z kodem QR) link oraz wpisanie tam danych, takich dzięki którymi atakujący będą próbowali wyprowadzić środki z rachunku ofiary. Wciąż bardzo duża skuteczność stosowanych przez cyberprzestępców technik manipulacji i wywierania wpływu na swoich ofiarach powoduje, że wszystkie jednostki zajmujące się ochroną klienta w sieci w tym CSIRT KNF na bieżąco śledzi i analizuje nowe sposoby działania oszustów, o których informuje za pośrednictwem mediów społecznościowych: **X** (**Twitter)**, **LinkedIn** oraz **Facebook**.

Aby poznać sposoby działania cyberprzestępców CSIRT KNF przygotował schematy ich działań, które publikujemy pod adresem:

https://cebrf.knf.gov.pl/encyklopedia-cyberbezpieczenstwa/schematy-oszustw.

Natomiast ze szczegółami kampanii przestępczych obserwowanych zarówno we wrześniu 2023 roku, jak i w 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 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*