Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

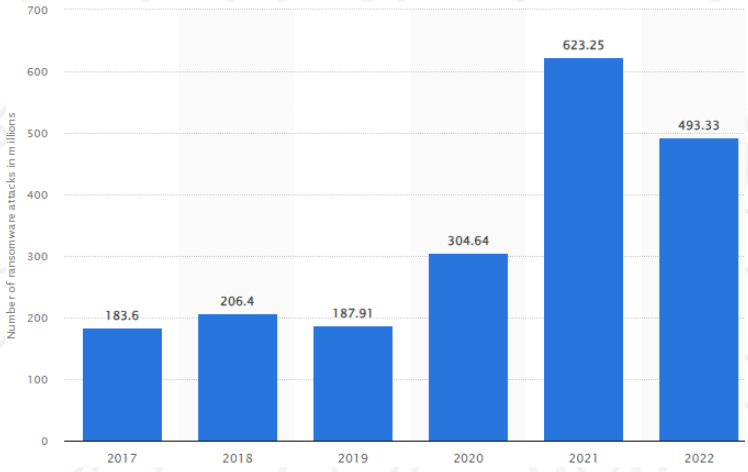
08/2023

Czarny rynek *Ransomware-as-a-Service* (RaaS) 3
Podrobione aplikacje komunikatorów *Telegram* i *Signal* trafiły do sklepów *Google Play* i *Galaxy Store* 4
Luki bezpieczeństwa w inteligentnych żarówkach marki *TP-Link oraz Tapo App* 5
Polski zespół '*Poland Can Into Space*' zajął 2 miejsce w zawodach *Hack-A-Sat* 6
Phishing-as-a-Service na wyższym poziomie: *Microsoft* alarmuje w związku z atakami adversary-in-the-middle (AiTM) 7
CERT Polska zasilił serwis haveibeenpwned.com danymi z kampanii phishingowej 8
Przedłużenie stopnia alarmowego CHARLIE-CRP 9
Kampanie przestępcze w sierpniu 2023 oczami *CSIRT KNF* 10
INFORMACJA O SZKOLENIACH 12
Oznaczenia TLP 13

Czarny rynek *Ransomware-as-a-Service* (RaaS)

Środowisko cyberprzestępcze cechuje się wysoką dynamiką zmienności. Obserwowane są częste zmiany nazw, łączenia i podziały grup. Do największych zaobserwowanych na przestrzeni lat, zorganizowanych grup zalicza się: *RYUK*, *Babuk*, *REvil*, *Conti*, *DarkSide*, *BlackMatter*, *BlackCat*. Wymienione podmioty cechują się świadczeniem usług typu *Ransomware-as-a-Service* (RaaS). Rozporoszona struktura oraz wirtualna, internetowa organizacja, przypominająca międzynarodowe korporacje utrudnia rozpracowanie ww. grup. Ponadto przyjęty model działalności polegający sprzedaży dostępu do oprogramowania oraz na wyciekach kodu źródłowego programów szyfrujących używanych przez największe gangi, powoduje powstawanie setek grup i tysięcy indywidualnych cyberprzestępców zajmujących się atakami typu ransomware. Należy zaznaczyć, że kod często jest udostępniany przez jego twórców za darmo, jak w przypadku *LockBit 3.0*, gdzie jego twórcy założyli własny program *bug bounty*, celem wyszukania i załatania podatności umożliwiających jego rozszyfrowanie przez służby. Ze względu na zaawansowane algorytmy szyfrowania (np. 256/512 bit lub RSA) luki w oprogramowaniu szyfrującym są często jedynym możliwym sposobem odtworzenia zasobów.

Według danych firmy *Fortinet* oprogramowanie *LockBit* (i wersje pochodne) odpowiadał za ponad 50% wszystkich światowych ataków tego typu w 2022 r. Natomiast eksperci z *statista.com*, stwierdzają, że ransomware stanowi 68% wszystkich zgłoszonych ataków i wyniósł ponad 155 mln ataków przy 493 mln próbach. Światowy czarny rynek ransomware w 2023 r. wyceniany jest na ok 8 bilionów dolarów.



Roczna, światowa liczba ataków typu ransomware (w mln.). Źródło: statista.com

Ransomware dostarczany jest zwykle na dwa sposoby – do osób indywidualnych i MŚP przez przesłanie spamu na skrzynki mailowe z wiadomościami phishingowych nakłaniającymi do kliknięcia w załączony, zainfekowany link. Natomiast do dużych firm, instytucji publicznych i podmiotów kluczowych przez zaawansowane ataki hackerskie (m.in. luki w infrastrukturze IT, przełamywanie systemów, phishing), po czym następuje umieszczenie implantu i rozpoczęcie szyfrowania.

***Rekomendacje**: najskuteczniejszą obroną przed ransomware jest podnoszenie świadomości użytkowników oraz utrzymywanie aktualnych i systematycznie wykonywanych odmiejscowionych kopii zapasowych, weryfikacja procedur ich użycia oraz regularna aktualizacja oprogramowania.*

*W przypadku podejrzenia ataku należy zgłosić próbę do CERT Polska na adres e-mail:**incydent.cert.pl** lub **cert@cert.pl**.*

*Więcej informacji znajdziesz w **Poradniku ransomware NASK** znajdującym się pod linkiem: https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf*

Źródła: *cert.pl, avlab.pl, bleepingcomputer.com, fortinet.com, statista.com*

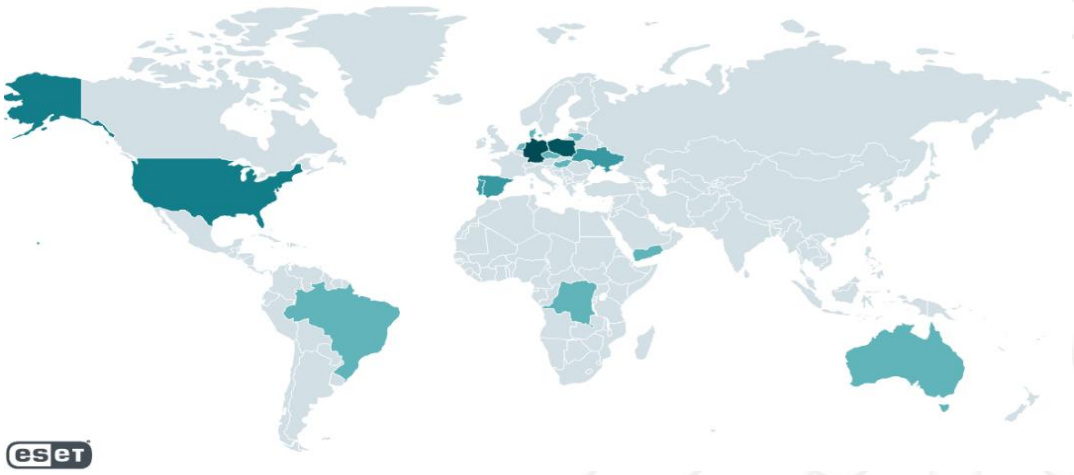
Podrobione aplikacje komunikatorów *Telegram* i *Signal* trafiły do sklepów *Google Play* i *Galaxy Store*

Badacze z firmy *ESET* wykryli i upublicznili kampanię złośliwego oprogramowania o nazwie *BadBazaar*. Wyżej wymienione narzędzie było dystrybuowane w oficjalnych sklepach *Google Play* i *Samsung Galaxy Store* oraz na dedykowanych stronach internetowych. *BadBazaar* został zaimplementowany w aplikacjach-podróbkach znanych komunikatorów, w wersjach przeznaczonych na urządzenia mobilne z systemem *Android*. Nosiły nazwy: *Signal Plus Messenger* (*Signal*) i *FlyGram (Telegram)* oraz reklamowane były jako bezpieczne, ulepszone wersje wskazanych komunikatorów.

Signal Plus Messenger – głównym zadaniem aplikacji było szpiegowanie komunikatora *Signal*. Oprogramowanie podszywając się pod aplikację *Signal* na smartphonie ofiary łączyło się po skanowaniu kodu QR z desktopowym klientem aplikacji, nadając dostęp do *Signala* użytkownikowi niezaufanemu.

Natomiast *FlyGram*, miało za zadnie pozyskiwanie wrażliwych informacji użytkownika dot. m.in. listy kontaktów, historię połączeń, kodu pin urządzenia, kopii zapasowych oraz listy zainstalowanych aplikacji. Ponadto dodatkowe nadanie uprawień umożliwiało pozyskanie listy kontaktów *Telegrama* oraz odczytanie treści wiadomości. W opinii Firmy *ESET* blisko 14 tys. użytkowników włączyło dodatkowe funkcje.

BadBazaar jest to rodzina złośliwego obramowania łączonego przez m.in. *NCCGroup*, *Lookout*, *Malpedia* z atrybucją chińskiej grupy APT15 (*Ke3chang*, *GREF*, *VixenPanda*). Trojan po raz pierwszy zaobserwowano w 2022 r. Używany był przez władze Chin wobec mniejszości Ujgurów. W opinii badaczy *ESET*, mimo wykrycia oprogramowania w telefonach obywateli wielu zachodnich państw (m.in.: USA, Australii, Niemiec, Kongo, Polski), nie byli oni grupą docelową ataku.



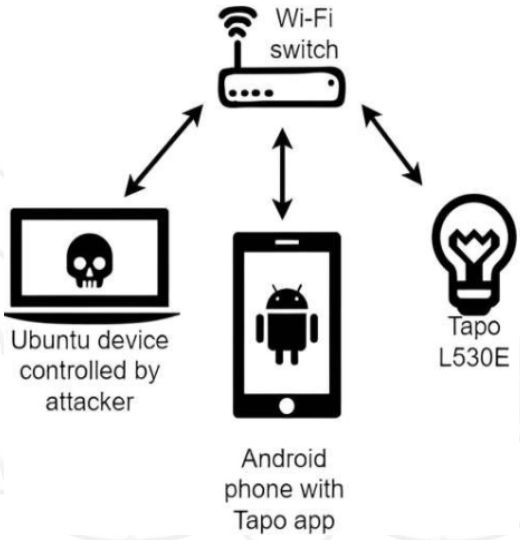
Mapa państw z wykrytymi zainfekowanymi urządzeniami. Źródło: welivesecurity.com

***Rekomendacje**: zawsze pobieraj aplikację z oficjalnych sklepów GooglePlay, GalaxyStore, AppStore itp., jednkaże każdoroazowo zwróć uwagę na dostawcę oprogramowania. Pobieraj tylko te, od oficjalnych dytrybutorów. Zachowaj szczególną ostrożność przy wersjach nazywanych „light", „plus", „lite", „new", „…24" .*

Źródła: eset.com, thehackernews.com, niebezpiecznik.pl, scmagazine.com, attack.mitre.org, welivesecurity.com

Luki bezpieczeństwa w inteligentnych żarówkach marki *TP-Link oraz Tapo App*

Urządzenia typu *Internet of Things* (IoT) stają się co raz bardziej popularne. Nawet najprostsze elementy wchodzące w skład tzw. *smart home*, jak inteligentne żarówki czy gniazdka elektryczne mogą stanowić wektor ataku dla cyberprzestępców. Badacze bezpieczeństwa z *Universita di Catania* wraz ze specjalistami z *University of London*, upublicznili cztery luki w zabezpieczeniach w jednym z najpopularniejszych modeli inteligentnych żarówek marki *TP-Link L530E* i aplikacji *Tapo*.



Połączenie z siecią. Źródło: arxiv.org

Do funkcjonalności takich żarówek zalicza się możliwość kontrolowania jej funkcji (m.in. wybór barwy światła, ustawienia włącznika czasowego czy możliwość monitorowania zużycia energii) za pomocą dedykowanej aplikacji na smartfona. Urządzenia tego typu łączą się z siecią za pośrednictwem routera domowej sieci Wi-Fi, co jest głównym powodem zainteresowania hakerów.

Odkryte luki wskazały zagrożenie na poziomie 7.6 i 8.8/10 zgodnie z *CVSS*, co sprawia że niebezpieczeństwo podatności jest wysokie oraz bardzo wysokie.

Pierwsza z nich pozwala atakującym na pozyskanie kluczy weryfikacyjnych metodą *brute force* lub poprzez dekompilację samej aplikacji *Tapo*. Druga natomiast, związana jest z nieprawidłowym uwierzytelnianiem żarówki, co powoduje możliwość podszycia się pod urządzenie, umożliwiając kradzież hasła *Tapo* i manipulację urządzeniem lub dalszy dostęp do sieci. Wejście do sieci prywatnej może powodować dostęp do wszystkich urządzeń do niej podłączonych, a co za tym idzie urządzenia mogą zostać zainfekowane i bez świadomości użytkownika stać się np. elementem botnetu i służyć jako koparki kryptowalut, prowadzić ataki typu DDoS, rozsyłać spam, funkcjonować jako VPS (*Virtual Private Server*) dla działań przestępczych, a w najgorszym przypadku powodować utartą danych dostępowych do urządzenia wraz z wypływem danych wrażliwych i prywatnych.

***Rekomendacje**: w każdym nowo uruchomianym urządzeniu należy zmieniać z domyślengo hasła porducenta na silne hasło własne, o kombinacji min. 12-14 znaków; stosować uwierzytelnianie wieloskładnikowe oraz wyłączanie produktów, które nie będą używane przez dłuższy czas. Dodatkowo należy pamiętać o najnowszych aktualizacjach zabezpieczeń, gdy tylko są dostępne. Powyższe czynności należy stpsować dla wszystkich inteligentnych urządzeń stosowanych w ramach smarthome jak: kamery internetowe, systemy bezpieczeństwa i kontroli, roboty sprzątające itp.*

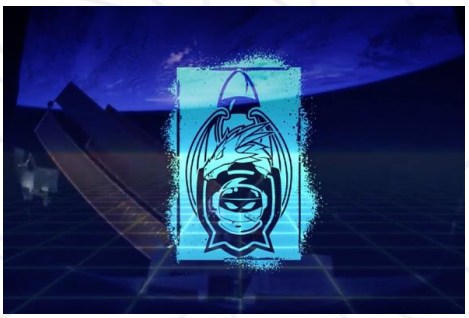
Zobacz więcej na temat polityki haseł:

https://www.gov.pl/web/baza-wiedzy/jak-tworzyc-bezpieczne-hasla
https://cert.pl/posts/2022/01/kompleksowo-o-haslach/

Źródła: *arxiv.org, malwarebytes.com, techxplore.com*

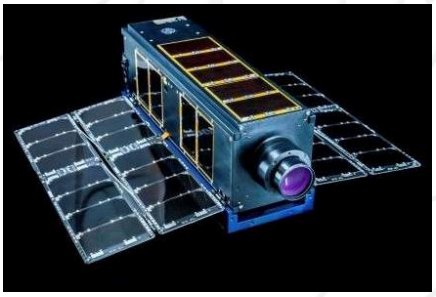
Polski zespół '*Poland Can Into Space*' zajął 2 miejsce w zawodach *Hack-A-Sat*

W tegorocznym konkursie *Hack-A-Sat* zespoły miały za zadanie włamać się do prawdziwego satelity wojskowego na orbicie. Był to pierwszy rok, w którym w konkursie zadaniem zespołów było zhakowanie rzeczywistego satelity lecącego nad Ziemią na żywo; w poprzednich latach wykorzystywano symulowane satelity na ziemi. Mały satelita-sześcian, znany jako *Moonlighter*, został opracowany przez *Aerospace Corporation* i *Laboratorium Badawcze Sił Powietrznych Stanów Zjednoczonych* i wystrzelony 5 czerwca 2023 roku na szczycie rakiety SpaceX Falcon 9 wraz z ładunkiem dla Międzynarodowej Stacji Kosmicznej. Zespoły miały za zadanie ominąć ograniczenia satelity dotyczące tego, które cele naziemne może obserwować, wydać mu polecenie zrobienia zdjęcia danego celu, a następnie przesłania tego zdjęcia do stacji naziemnej.



Logo grupy Poland Can Into Space, Źródło:hackasat.com

Pięć drużyn rywalizowało w konkursie *Hack-A-Sat* trwającym od 11 do 14 sierpnia w ramach corocznej konwencji hakerskiej *DEF CON* w Las Vegas. W tym roku zwycięskim zespołem została „*mHACKeroni*" – grupa składająca się z członków pięciu włoskich zespołów zajmujących się badaniami cybernetycznymi. **Polski zespół zajął prestiżowe 2 miejsce w tych międzynarodowych zawodach, co stanowi duże osiągnięcie i dowodzi świetnych umiejętności członków zespołu.**



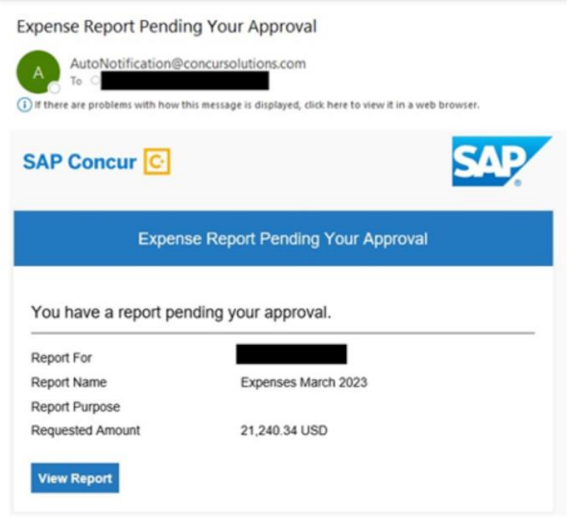
Mały satelita Moonlighter wykorzystany w tegorocznej edycji konkursu Hack-A-Sat, Źródło: aerospace.org

Organizując zawody takie jak *Hack-A-Sat*, *Siły Powietrzne Stanów Zjednoczonych i Dowództwo Systemów Kosmicznych Stanów Zjednoczonych* mają na celu identyfikację słabych punktów, które można wykorzystać do poprawy bezpieczeństwa systemów satelitarnych. Ma to istotne znaczenie z uwagi na zwiększoną liczbę ataków hakerskich (przykładem ostatnie cyberataki na satelity *Starlink SpaceX*, które uległy intensyfikacji po inwazji Rosji na Ukrainę).

Źródła: spidersweb.pl, space.com, hackasat.com, aerospace.org

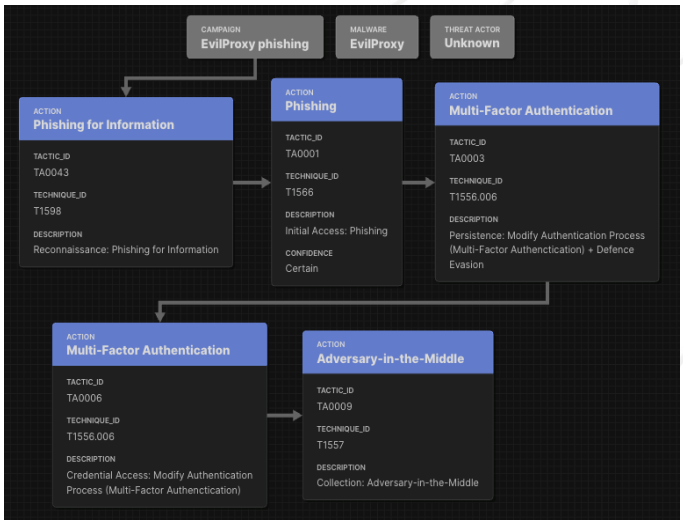
Phishing-as-a-Service na wyższym poziomie: *Microsoft* alarmuje w związku z atakami adversary-in-the-middle (AiTM)

Kampania phishingowa wykorzystująca platformę *EvilProxy* była skierowana do ponad 120 000 użytkowników pakietu *Microsoft Office 365* (Microsoft 365). *EvilProxy* to platforma typu **Phishing-as-a-Service**, która wykorzystuje reverse proxy do przekazywania wielu żądań uwierzytelniania MFA (multi-factor authentication) i kradnie dane uwierzytelniające użytkowników oraz pliki cookie sesji (session cookies). Jeśli dana usługa wymaga MFA, oszuści mogą wykorzystać reverse proxy do przechwycenia żądań MFA od ofiary. Następnie mogą próbować przekierować te żądania na swoje własne kontrolowane serwery MFA). To rosnące zagrożenie łączy w sobie wyrafinowane techniki phishingu typu **Adversary-in-the-Middle**, z zaawansowanymi metodami przejmowania kont w odpowiedzi na rosnące wykorzystanie uwierzytelniania wieloczynnikowego przez organizacje.



Przykładowy phishingowy e-mail z próbą podszycia się pod firmę SAP Concur. Źródło: proofpoint.com.

Atakujący podszywali się pod marki takie jak *Adobe*, *DocuSign* i *Concur*, a także wykorzystywali otwarte przekierowania, aby uniknąć wykrycia. Po skompromitowaniu konta *Microsoft 365*, cyberprzestępcy zyskują stały dostęp (persistence), dodając własną metodę MFA. Kampania udanych incydentów przejęcia kont w chmurze dotknęła przede wszystkim kadrę kierowniczą wysokiego szczebla w ok. 100 organizacjach.



Przykładowy schemat ataku na podstawie MITRE oraz dostępnych informacji, źródło: opracowanie własne

Platforma *EvilProxy* jest sprzedawana cyberprzestępcom za 400 dolarów miesięcznie. Cyberprzestępcy stojący za kampanią są na chwilę obecną nieznani, jednakże można przypuszczać, że stoi za nimi powiązana z Rosją grupa *Callisto* (która stosowała podobne ataki w przeszłości). Wzrost platform takich jak *EvilProxy*, stwarza poważne zagrożenie, dlatego organizacje powinny nadać wysoki priorytet zwiększaniu świadomości pod kątem cyberbezpieczeństwa, wdrożyć silniejsze zasady filtrowania poczty e-mail oraz używać kluczy fizycznych (np. *Yubikey*).

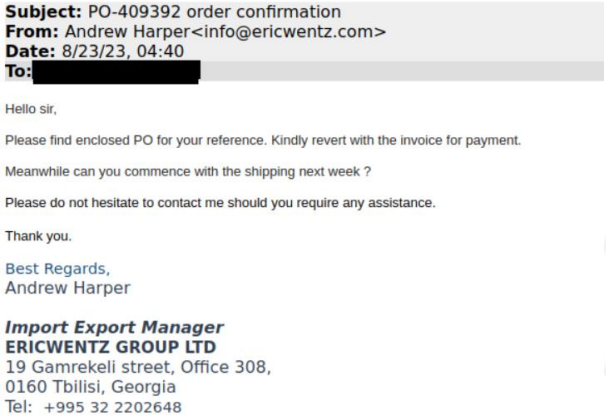
Zobacz więcej: *https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/*

Źródła: bleepingcomputer.com, infosecurity-magazine.com, proofpoint.com, microsoft.com

CERT Polska zasilił serwis haveibeenpwned.com danymi z kampanii phishingowej

W ramach jednej z ostatnich kampanii phishingowych przestępcy zebrali dane uwierzytelniające do 68 tys. skrzynek pocztowych osób z całego świata. Zespołowi *CERT Polska* w sierpniu br. udało się uzyskać listę ofiar i w związku z globalnym charakterem wycieku, dane te zostały przekazane do serwisu *Have I Been Pwned*.

W ramach kampanii zbierano adresy e-mail i hasła za pośrednictwem wiadomości phishingowej udającej potwierdzenie zakupu. Próba oszustwa rozpoczynała się od typowego maila z prośbą o więcej informacji. W tym przypadku mail zawierał załącznik fałszywego zamówienia zakupu, w którym żądano danych logowania, które następnie przesyłano z powrotem do infrastruktury kontrolowanej przez atakującego. *CERT Polska* zidentyfikował kolejne 202 inne kampanie phishingowe działające na tym samym serwerze C2, który został obecnie wyłączony.


Subject: PO-409392 order confirmation
From: Andrew Harper<info@ericwentz.com>
Date: 8/23/23, 04:40
To: [redacted]

Hello sir,

Please find enclosed PO for your reference. Kindly revert with the invoice for payment.

Meanwhile can you commence with the shipping next week ?

Please do not hesitate to contact me should you require any assistance.

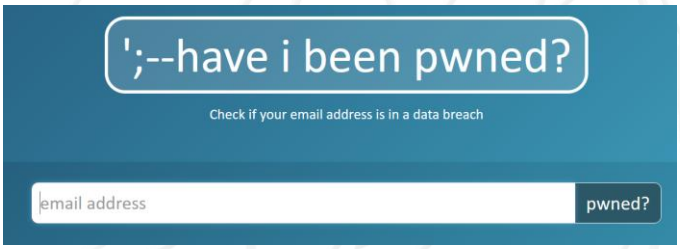
Thank you.

Best Regards,
Andrew Harper

Import Export Manager
ERICWENTZ GROUP LTD
19 Gamrekeli street, Office 308,
0160 Tbilisi, Georgia
Tel: +995 32 2202648

Przykładowa wiadomość phishingowa w ramach kampanii obserwowanej przez CERT Polska, źródło: TroyHunt.com

Have I Been Pwned jest to serwis pozwalający sprawdzić, czy dane użytkownika zostały przejęte w ramach licznych wycieków. Od 2013 r. portal zbierane informacje o wyciekach, dzięki czemu dysponuje obszerną bazą i uchodzi za wiarygodne źródło. Przekazanie danych serwisowi może pozwolić ocalić wiele osób przed byciem ofiarę cyberprzestępców.



Strona główna serwisu Have I Been Pwned, źródło: haveibeenpwned.com

***Rekomendacje**: W celu zwiększenia swojego bezpieczeństwa warto także włączyć uwierzytelnianie dwuskładnikowe, korzystać z menedżerów hasał, używać różnych haseł do różnych portali, stosować odpowiednio długie i złożone hasła. Nie powinno się też otwierać załączników oraz klikać w linki zawarte w podejrzanych mailach.*

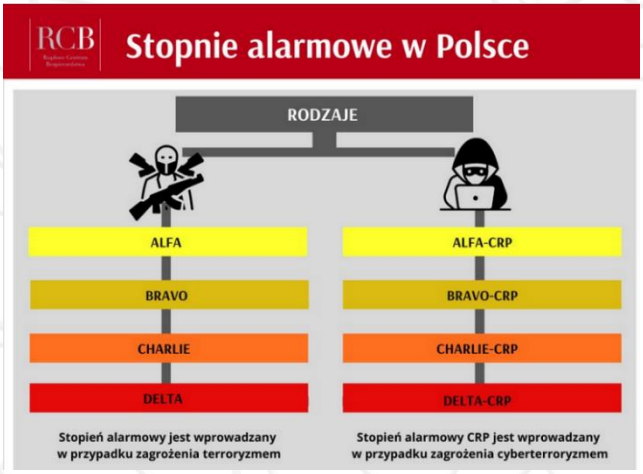
Przypominamy także o istnieniu rządowego serwisu BezpieczneDane.gov.pl, który powstał w związku upublicznieniem pod koniec maja br. loginów i haseł części polskich użytkowników internetu. Korzystając z wyszukiwarki na tej stronie możesz dowiedzieć się, czy Twoje dane mogły trafić w ręce cyberprzestępców. Planowane jest uzupełnianie bazy o dane z nowopojawiających się wycieków. Jeśli Twoje dane wyciekły przeskanuj swój komputer antywirusem, zmień swoje hasło korzystając z bezpiecznego komputera i monitoruj aktywność na swoich kontach.

Źródła: *NASK, haveibeenpwned.com, TroyHunt.pl.*

Przedłużenie stopnia alarmowego CHARLIE-CRP

Ponownie przedłużone zostały stopnie alarmowe ogłaszane na podstawie ustawy o działaniach antyterrorystycznych. Ustawa ta wprowadziła 4-stopniowy system stopni alarmowych na wypadek zagrożeń terrorystycznych oraz stopni alarmowych w cyberprzestrzeni (CRP).

W związku z sytuacją bezpieczeństwa w regionie, w tym inwazją Rosji na Ukrainę oraz działaniami hybrydowych Rosji i Białorusi, od 21 lutego 2022 r. na terytorium RP obowiązuje trzeci stopień alarmowy CHARLIE-CRP. Jednocześnie obowiązuje także drugi stopień alarmowy (BRAVO) dla zagrożeń terrorystycznych. Stopnie te są cyklicznie przedłużane.



Źródło: RCB

Zgodnie z ostatnimi zarządzeniami premiera na całym terytorium RP przedłużono obowiązywanie obu stopni alarmowych, tym razem na okres od 01.09 – 30.11.2023 r. Co istotne w kontekście zapewnienia cyberbezpieczeństwa procesu wyborczego, **stopień CHARLIE-CRP obejmie także nadchodzące wybory parlamentarne**, które odbędą się 15 października.

Zgodnie z ustawą stopnie CRP są wprowadzane w przypadku zagrożenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej.

Rozporządzenie premiera z 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP określa szczegółowe zakresy przedsięwzięć wykonywanych przez organy administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego, w tym we współpracy z operatorami infrastruktury krytycznej. Przy obowiązywaniu stopnia CHARLIE-CRP należy wykonać zadania przewidziane w rozporządzaniu dla stopni ALFA-CRP i BRAVO-CRP, ponadto należy wykonać w szczególności następujące zadania:

1) wprowadzić całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów;
2) dokonać przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w przypadku zaistnienia ataku;
3) przygotować się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku, w tym:
   a) dokonać przeglądu i ewentualnego audytu planów awaryjnych oraz systemów,
   b) przygotować się do ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamknięcia.

Zobacz więcej: *https://www.gov.pl/web/rcb/przedluzenie-obowiazywania-stopni-alarmowych-do-30-listopada-2023-r*

Źródła: MSWiA, RCB.

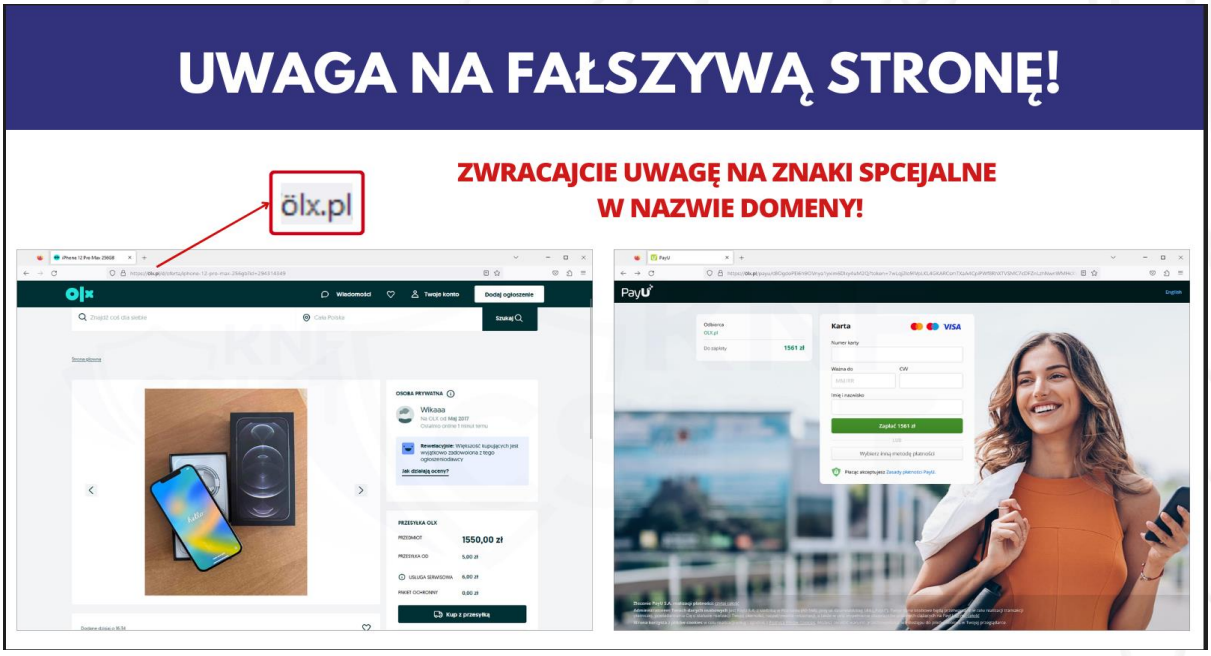
Kampanie przestępcze w sierpniu 2023 oczami *CSIRT KNF*

Cyberprzestępcy nie mają wakacji i nieustannie wymyślają nowe kampanie, aby wyłudzić od użytkowników ich dane osobowe, dane uwierzytelniające do bankowości elektronicznej czy dane kart płatniczych. Ich wzmożoną aktywność w sierpniu 2023 r. pokazują również statystyki wykrytych niebezpiecznych domen. Dzięki podjętym działaniom *CSIRT KNF* zgłosił do zablokowania 2 244 domeny (1 725 w lipcu), dla porównania *CERT Polska* dodał na listę ostrzeżeń 6 992 domeny (4 693 w lipcu). Obecnie na liście ostrzeżeń przed niebezpiecznymi stronami (*CERT HOLE*) znajduje się 137 459 domen.

Każda osoba poruszająca się w Internecie niezależnie od tego z jakiej wyszukiwarki korzysta (*Google*, *Bing* czy *MSN*) mogła już trafić na reklamy oferujące rzekomy niebagatelny zysk, w bardzo krótkim czasie, czy możliwość wygrania pieniędzy biorąc udział w ankiecie prowadzonej przez instytucję finansową czy spółkę skarbu państwa. Kampanie te miały miejsce także w sierpniu 2023 r. Jedną z nich była umieszczona przez cyberprzestępców w wyszukiwarce *Google* reklama, podszywająca się pod stronę banku *PKO BP*. Po wejściu na stronę byliśmy informowani, że Bank prowadzi ankietę dotyczącą badania jakości obsługi klienta. Wystarczyło odpowiedzieć na parę pytań z ankiety i podać swoje dane osobowe, aby otrzymać nagrodę pieniężną.

Kolejna kampania phishingowa dystrybuowana była przez reklamy, ale na platformie *Facebook*. Podszywając się pod firmę telekomunikacyjną *ORANGE POLSKA*, pod pretekstem możliwości otrzymania doładowania telefonu na kartę oraz pakietu Internetu, oszuści zachęcali do kliknięcia w link. Następnie ofiara przekierowywana była do strony phishingowej, na której należało podać numer telefonu, adres e-mail, aktywny kod *BLIK* oraz dane karty płatniczej.

Cyberprzestępcy przygotowali również kampanię, w której podszywali się pod jeden z wiodących portali sprzedażowych. To co ciekawe w tej kampanii, atakujący wykorzystali dawno nieobserwowaną metodę maskowania nazwy fałszywej strony, tzw. „*punycode*”. Polegała ona na tym, że w adresie strony zmienili jedną z liter "o", na „ö” co na pierwszy rzut oka



utrudniało użytkownikowi weryfikację jej poprawności (rysunek). Po kliknięciu w link osoba chcąca dokonać zakupu podawała dane swojej karty płatniczej oraz kod *BLIK* do autoryzacji transakcji.

Kolejną kampanią, która w sierpniu 2023 r. przybrała na sile były rozsyłane przez cyberprzestępców SMS-y o treści *„Mamo – spadł i rozwalił mi się telefon, skontaktuj się ze mną na WhatsApp”*. Ofiara, która dała się nabrać na takiego SMS-a, kontaktowała się z oszustem na komunikatorze, gdzie otrzymywała prośbę o opłacenie faktury za zakup nowego telefonu z podanym numerem rachunku bankowego i kwotą do uiszczenia.

Pewną nowością jest też wykorzystywanie przez cyberprzestępców nowej funkcji komunikatora *WhatsApp*, umożliwiającą zdalne wyświetlanie ekranu. Dzięki temu w trakcie oszustwa dokładnie widzą wszystko, co ofiara robi na swoim telefonie. Wcześniej wykorzystywali w tym celu dedykowane aplikacje do pomocy zdalnej, które wymagały oddzielnej instalacji. Wykorzystanie komunikatora *WhatsApp* eliminuje konieczność wytłumaczenia poszkodowanemu jak ma zainstalować oraz uruchomić dodatkowe narzędzie.

Skuteczność stosowanych przez cyberprzestępców technik manipulacji i wywierania na swoich ofiarach presji czasu i emocji jest wciąż bardzo duża. *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 w sierpniu 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*