



Ministerstwo
Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:GREEN

BIULETYN INFORMACYJNY

ZAGROŻENIA W CYBERPRZESTRZENI

02/2024





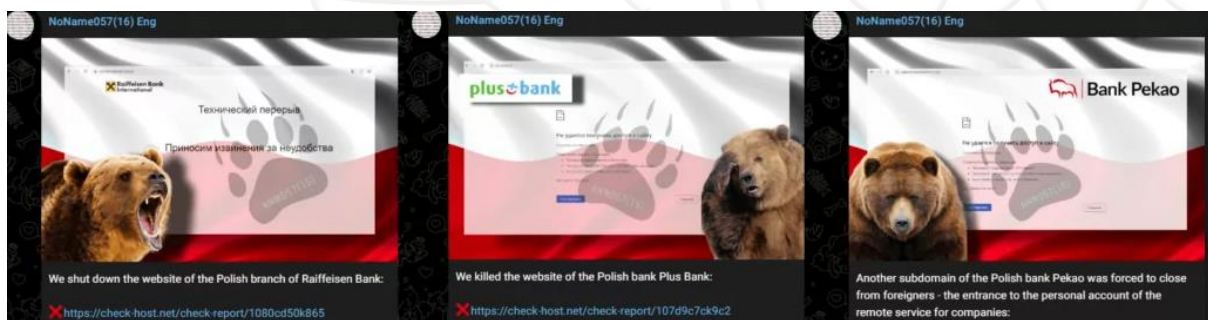
SPIS TREŚCI

<i>Krajobraz rosyjskich działań w cyberprzestrzeni dwa lata od eskalacji wojny na Ukrainie</i>	<i>3</i>
<i>Zagrożenia w cyberprzestrzeni mogą wpływać na wybory?</i>	<i>5</i>
<i>Jak uniknąć nieproszonych gości w trakcie wideokonferencji</i>	<i>7</i>
<i>Wspólna akcja CISA oraz partnerów zagranicznych w tym SKW przeciwko grupie APT28.....</i>	<i>8</i>
<i>LolekHosted, Lockbit i Centralne Biuro Zwalczania Cyberprzestępczości w Operacji „CRONOS”</i>	<i>9</i>
<i>Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta.....</i>	<i>12</i>
<i>INFORMACJA O SZKOLENIACH</i>	<i>14</i>
<i>Oznaczenia TLP.....</i>	<i>15</i>



Krajobraz rosyjskich działań w cyberprzestrzeni dwa lata od eskalacji wojny na Ukrainie

W dniu 24 lutego 2024 roku obchodziliśmy niechlubną, już drugą rocznicę pełnoskalowej napaści zbrojnej Federacji Rosyjskiej na Ukrainę. W mediach głównego nurtu, jak i sieciach społecznościowych codziennie otrzymujemy informacje dotyczące starć między stronami konfliktu. Obrazy brutalnych walk, działań ciężkiej techniki wojskowej, wywiady reporterskie prosto z okopów, zdjęcia rannych i poległych żołnierzy oraz ujęcia efektownych wybuchów i generowanych przez nie zniszczeń wzmocniają przekaz dostarczany przez redaktorów. Wymienione elementy pozwalają nam uzmysłować sobie skalę działań zbrojnych. Dzięki temu, choć na chwilę możemy przenieść się na linię frontu, by w minimalnym stopniu pojąć niebezpieczeństwo wojny i zrozumieć skutki jakie może za sobą nieść dla nas, czy naszych bliskich. Audiowizualna dokumentacja zdarzeń ułatwia nam podjąć próbę zrozumienia wojny, gdyż bezpośrednio wpływa na nasze zmysły. Obraz i dźwięk uruchamiają wyobraźnię, wywołują emocje oddziałujące na nasze postawy i postrzeganie świata... w ten oto sposób, powyższym, nieco rozbudowanym wstępem połączyliśmy świat rzeczywisty ze sferą informacyjną. Ta druga jest częścią wirtualną naszej rzeczywistości. Jednak obecnie nierozłącznie związaną z tą pierwszą.



Screeny z informacjami o atakach dokonanych przez grupę NoName057(16).

Źródło. SOCRadar

Sferę informacyjną możemy podzielić na dwie podstawowe płaszczyzny. Pierwsza, czyli klasycznie rozumiana przestrzeń wymiany informacji o otaczającym nas świecie – informacji dochodzących do odbiorców końcowych (m.in. treści w sieciach społecznościowych, newsy, tj. przetworzony i gotowy do odczytu materiał informacyjny). Druga, to płaszczyzna cyfrowa służąca do wymiana niewyobrażalnych ilości danych i informacji w formie cyfrowej będącej krwioobiegami procesów informatycznych. Oparta jest o zaawansowaną fizyczną infrastrukturę techniczną i procesy logiczne umożliwiające funkcjonowanie technologiczne świata jaki znamy. Skala wielkości środowiska technicznego oraz zaawansowanie procesów w nim zachodzących są trudne do zobrazowania i wyobrażenia. Powoduje to ogromne problemy przy próbie uzmysłwienia nietechnicznym odbiorcom wagi i znaczenia cyberprzestrzeni dla dzisiejszego świata. Jednakże Rosjanie, jak i Ukraińcy mają świadomość jej znaczenia, co możemy obserwować w odbywającej się równolegle do linii frontu (przez co dla większości ludzi mało atrakcyjnej i trudnej do zrozumienia) „niewidzialnej wojnie” w przestrzeni cyfrowej, w której my, jako Polska również uczestniczymy.



Od początku 2022 r. Ukraina jak i państwa ją wspierające zmagają się ze wzmożonymi, wrogimi działaniami w cyberprzestrzeni. Trzeba dodać, że okres dwóch minionych lat charakteryzuje się skokowym rozwojem rozwiązań i procedur bezpieczeństwa teleinformatycznego Polski oraz wzrostem świadomości administracji publicznej, jak i dużego biznesu w zakresie cyberbezpieczeństwa. Dotyczy to konieczności rozwoju infrastruktury IT, co bezpośrednio wpływa na poziom bezpieczeństwa zasobów i procesów polskiej sfery cyfrowej. Jednak rozwój ten, spowodowany jest przede wszystkim wyścigiem zbrojeń w cyberprzestrzeni i reakcją na powstające zagrożenia. Nowe ataki powodują nowe zabezpieczenia, a nowe zabezpieczenia wpływają na tworzenie nowych metod, dobór celów i narzędzi ataków. Wygrywa ten, kto jest w stanie zapewnić większe zasoby sprzętowe, finansowe, technologiczne, a przede wszystkim ludzkie.

I tak, w ciągu dwóch lat zaobserwowano wyraźny wzrost zagrożeń stosowanych wobec Polski. Wrogą aktywność jednoznacznie przypisuje się aktywności grup hakerskich związanych bezpośrednio z rosyjskimi oraz białoruskimi podmiotami państwowymi (m.in. grupy APT28 i APT29). Ugrupowania te, wykorzystują zaawansowane techniki i metody prowadzonych ataków. Cechują się dużym kunsztem technicznym i tzw. OPSEC'kiem oraz doбором wysoce wrażliwych i intratnych celów związanych m.in. z infrastrukturą krytyczną, sektorem obronnym, czy klasą polityczną. Działania te, świadczą o wsparciu instytucjonalnym ww. grup, co widoczne jest w posiadanych potencjale i zasobach, niedostępnych dla tzw. samotnych wilków i grup cyberprzestępczych. Jednakże, wroga działalność „wschodnich” grup APT od dawna stanowi zagrożenie zamieszczane w ocenach ryzyka dla kluczowych podmiotów publicznych. Swoistym novum, zaobserwowanym w ciągu dwóch ostatnich lat, jest skala ruchów hakywistycznych (np. *KillNet*, *NoName057(16)*). Ich cele są spójne z polityką wrogich państw, jednak zasada ich działania i organizacji opiera się na „oddolnych” i „ideologicznie słusznych” inicjatywach społeczności internetowych (a same grupy są sterowane przez służby specjalne ww. krajów). Grupy hakywistyczne wykorzystują stosunkowo proste metody i łatwo dostępne narzędzia prowadzenia wrogiej aktywności. Skupiają się na stosowaniu ataków typu DDoS. W działaniach wykorzystują botnety - własne i komercyjnie, nielegalnie dostępne w *darknecie* oraz moce obliczeniowe urządzeń udostępnionych przez członków własnej, ideologicznie im bliskiej społeczności. Do celów ataków głównie zalicza się podmioty ze sfery wrażliwej dla obywateli, tj. odbiorów informacji medialnej – czyli grupy atakują m.in. bankowość, infrastrukturę krytyczną i łańcuchy dostaw. Ataki te, często nieskuteczne, mogą utrudnić funkcjonowanie danej organizacji oraz spowodować szkody wizerunkowe. Przy skutecznie prowadzonej polityce informacyjnej przez grup hakywistyczne stanowi to element w sferze propagandowej, dla promowania własnych działań i szerzenia dezinformacji wrogich nam państw przy zasięgach medialnych znacznie przerastających faktyczną szkodliwość ataków.

Powyższy opis nie wyczerpuje wszystkich negatywnych trendów i zagrożeń obserwowanych w krajowej cyberprzestrzeni, lecz przedstawia tylko te z powszechnie obserwowanych.



Zagrożenia w cyberprzestrzeni mogą wpływać na wybory?

Państwa demokratyczne muszą odnaleźć się w dobie przemian cywilizacyjnych. Na przykładzie obecnej transformacji polskiego sektora publicznego, można uznać iż wymaga ona otwarcia się na usługi cyfrowe poprzez wdrażanie ich dostępności w szerokim zakresie i na wielu płaszczyznach funkcjonowania administracji państwa. Podstawowe funkcje urzędów oraz ich zadania przechodzą do sfery cyfrowej. Sama dostępność usług cyfrowych wzrasta skokowo z każdym kolejnym rokiem, co można zauważyć po np. rozwoju funkcjonalności *mObywatela*. Dużą część spraw urzędowych można obecnie przeprocesować poprzez dedykowane platformy cyfrowe wskazanych instytucji publicznych. I póki co... nie widać przesłanek świadczących o możliwym odwróceniu tego trendu. Przy tak opisanej perspektywie rozwoju, należy stwierdzić, że państwa będą oferować obywatelom szeroki wachlarz kolejnych usług elektronicznych. Skokowy rozwój społeczeństwa cyfrowego oraz digitalizacji administracji publicznej może w końcu stawić wyzwanie *clue* demokracji jakim jest organizacja wyborów powszechnych.

Przeprowadzenie wyborów z uwzględnieniem głosowania elektronicznego wiąże się z nowymi wyzwaniami dla bezpieczeństwa i rzetelności całego procesu wyborczego. Stanowi on o wiarygodności państwa, stabilności jego systemu oraz dojrzałości demokracji i społeczeństwa.

Obecnie sam proces zbierania i liczenia głosów jest bezpieczny ze względu na swoją mocno... analogową formę, opartą o klasyczne karty do głosowania. Jednakże, patrząc na proces prowadzenia wyborów prezydenckich w Stanach Zjednoczonych w latach 2016 i 2020, trzeba stwierdzić, że obecne zagrożenie jest przede wszystkim w sferze informacyjnej. Obrazują to próby ingerencji Rosji w wyniki wyborów przy wykorzystaniu narzędzi i metod walki informacyjnej w cyberprzestrzeni. Jak podaje STC NATO Rosja była odpowiedzialna nie tylko za zakłócenie wyborów w USA w 2016 r., ale również za m.in. referendum w sprawie *Brexitu* i późniejszych wyborów parlamentarnych w UK, Niemczech, Francji w 2017 r. oraz w referendum w sprawie statusu hiszpańskiej Katalonii.

Wpływ Rosjan we wspomnianych kampaniach dotyczył przede wszystkim oddziaływania na nastroje społeczne oraz chęć kreowania przychylnych swoim interesom postaw i opinii publicznych. Do wymienionych działań wykorzystano m.in. ośrodki dezinformacji, inspiracji, PRu, marketingu politycznego i algorytmów sieci społecznościowych.

Patrząc na obecną sytuację geopolityczną można wnioskować, iż nie tylko Rosja, ale również Chiny, Kora Płn., i Iran należą do grupy krajów mogących mieć interes w zakłócaniu procesów wyborczych lub wpływie na sam rezultat wyborów. Celem nadrzędnym nie jest bezpośredni wpływ na wynik, ale jego podważanie i powodowanie rosnących konfliktów społecznych. W ciągu ostatnich lat zaobserwowano wzrost ataków na procesy wyborcze w państwach nie tylko szeroko rozumianego Zachodu, ale również w m.in. Tybecie, Tajwanie oraz krajach byłego Bloku Wschodniego (Ukraina, Mołdawia, Gruzja).

Na podstawie obserwacji i analizy bieżących trendów walki informacyjnej w cyberprzestrzeni, można przypuszczać o potencjalnym zastosowaniu przez służby specjalne ww. państw



najnowszych technologii, których dostępność oraz możliwości wzrosły wykładniczo w czasie ostatnich kilku lat.

Do narzędzi prawdopodobnych do wykorzystania zaliczyć trzeba m.in.: kampanie phishingowe, przejęcia stron, kont i portali internetowych, publikacje danych wrażliwych, ataki na dostępność usług (DoS i DDoS), audiowizualne *Deep Fake*'i, generatywną AI, czy kampanie dezinformacyjne w mediach społecznościowych przy wykorzystaniu tysięcy fikcyjnych kont zarządzanych przez AI oraz symulujących prawdziwych użytkowników tworząc tzw. zasięgi i wpływając na szeroko rozumianą opinię publiczną w atakowanych krajach.

Warto zauważyć, że ataki wymierzone w proces wyborczy nie muszą przyjmować wyrafinowanej formy. Prosta manipulacja treściami zmieszanymi w social mediach, czy zwykłe zablokowanie możliwości sprostowania natychmiastowego kontrowersyjnych treści są bardzo skuteczne.



Wybory w Polsce.
Źródło: stockphoto.com

Rok 2024 w Polsce jest rokiem wyborczym. Wybory samorządowe odbędą się 7 kwietnia. Natomiast druga tura jest przewidziana na dzień 21 kwietnia 2024 r. To nie koniec. 9 czerwca w naszym kraju odbędą się wybory do Parlamentu Europejskiego.

Należy jednak zaznaczyć, że to na aparacie publicznym spoczywać będzie sam, całkowity ciężar zabezpieczenia wyborów przed zagrożeniami cyberbezpieczeństwa oraz odpowiedzialności za potencjalne naruszenia przebiegu procesu wyborczego

Instytucją wiodącą w zakresie bezpieczeństwa wyborów, zgodnie z przepisami *ustawy o krajowym systemie cyberbezpieczeństwa* oraz *ustawy o Agencji Bezpieczeństwa Wewnętrznego* oraz *Agencji Wywiadu*, jest Agencja Bezpieczeństwa Wewnętrznego, z którą Ministerstwo Cyfryzacji współpracuje w ramach krajowego systemu cyberbezpieczeństwa. ABW oraz działający w ramach tej instytucji CSIRT GOV podjęło już szereg działań mających na celu podniesienie bezpieczeństwa wyborów w kontekście działań w cyberprzestrzeni.

Ponadto zgodnie z *ustawą o krajowym systemie cyberbezpieczeństwa* działania te leżą w zakresie kompetencji Zespołów Reagowania na Incydynty Bezpieczeństwa Komputerowego (CSIRT) poziomu krajowego. CSIRT-y poziomu krajowego odpowiadają m.in. za monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym (art. 26 ust. 3 pkt 1).

Wyżej wymienione wydarzenia wymagają wzmożonej czujności nie tylko instytucji odpowiedzialnych za ich efektywne i bezpieczne przeprowadzenie, ale również nas. Wyborców. Co świadczy o naszej odpowiedzialności społecznej.

Źródła: gazetaprawna.pl, nask.pl, dw.com, portalsamorzadowy.pl, cyberdefence24.pl, journals.umcs.pl



Jak uniknąć nieproszonych gości w trakcie wideokonferencji

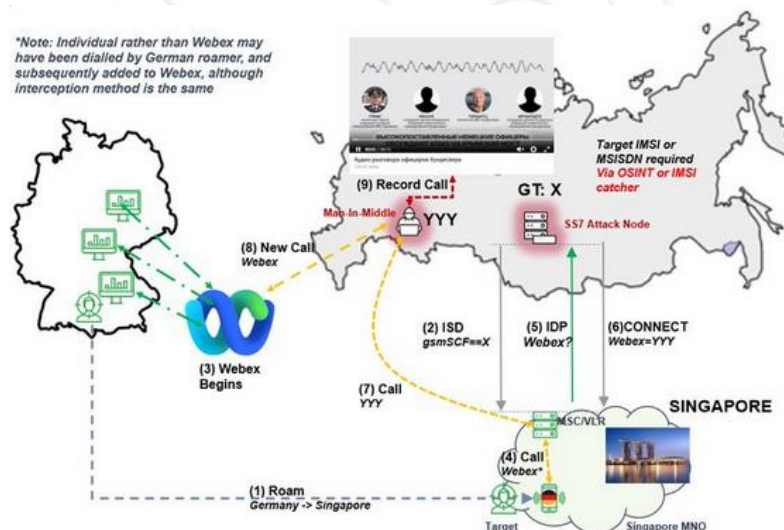
Świat obiegła wieść o podsłuchanej przez Rosjan wideokonferencji niemieckich generałów, którzy dyskutowali o sytuacji na Ukrainie, w tym m.in. na temat możliwości przekazanie Ukrainie pocisków manewrujących dalekiego zasięgu *Taurus*.

Rozmowa miała miejsce na ogólnodostępnej platformie *Webex*, do której podłączyli się Rosjanie. Następnie nagranie ze spotkania zostało przez nich udostępnione na kanale RT, czyli kremlowskiej tubie propagandowej. Sprawa jest kompromitująca nie tylko z uwagi na treść rozmów, ale przede wszystkim na fakt podsłuchania rozmowy. Wedle pojawiających się przypuszczeń do przechwycenia komunikacji mogło dojść, gdyż jeden z uczestników spotkania podłączył się poprzez hotelowe wifi w Singapurze. Świadczy to więc o braku stosowania zasad cyberhigieny przez użytkowników. Jednak jest też znacznie bardziej poważniejszy systemowy problem braku wykorzystania specjalnych środków łączności zapewniających bezpieczeństwo, zarówno do komunikacji jawnej (ale wrażliwej), jak również niejawnej o odpowiedniej klauzuli tajności.

Być może *Bundeswehra* i niemiecka administracja rządowa dysponują takimi środkami, ale nie zdecydowano się ich użyć z uwagi na nieodpowiedzialne wygodnictwo (co nie jest tylko problemem oficjeli w tym kraju). Często politycy nie korzystają z łączności specjalnej, bo wiąże się z posiadaniem dodatkowego urządzenia (lub urządzeń) i dopełnianiem procedur bezpieczeństwa. Ważne jest także odpowiednie nasycenie tego typu środkami, aby były one dostępne dla odpowiedniego kręgu osób, które powinny mieć do nich dostęp.

W Polsce na potrzeby administracji rządowej i Krajowego Systemu Cyberbezpieczeństwa Ministerstwo Cyfryzacji wdrożyło [bezpieczny komunikator](#) dostępny na urządzeniach służbowych. Ponadto na potrzeby łączności niejawnej Ministerstwo Cyfryzacji zleciło NASK-PIB opracowanie systemu [SKR-Z](#) (obecnie już wykorzystywanego), stanowiącego wersję rozwojową systemu *CATEL* opracowanego przez ABW. Ministerstwo Cyfryzacji, także jako zadanie zlecone NASK-PIB, zapewnia sprzęt i urządzenia ICT do komunikacji niejawnej w ramach [Projektu Połączonego Centrum Operacyjnego Cyberbezpieczeństwa \(PCOC\)](#). Spotkania koordynacyjne PCOC służą do bieżącego zarządzania bezpieczeństwem polskiej cyberprzestrzeni i umożliwiają sprawne reagowanie na zagrożenia.

Źródła: *Pravda.com.ua*, *Politico*, *Recorded Future*, NASK, @mcdaidc (X)



Źródło możliwego wycieku. Źródło: @mcdaidc (X)



Wspólna akcja CISA oraz partnerów zagranicznych w tym SKW przeciwko grupie APT28

27 lutego 2024 r. amerykańska agencja CISA (Agencja ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury) wydała publikację pt: „Rosyjscy cyberprzestępcy wykorzystują zainfekowane routery do ułatwiania operacji w cyberprzestrzeni”. FBI, NSA, US Cyber Command i międzynarodowi partnerzy ostrzegają przed wykorzystywaniem przez rosyjskie grupy cyberprzestępcze sponsorowane przez państwo skompromitowanych routerów *Ubiquiti EdgeRouters* (EdgeRouters) do przeprowadzania ataków hakerskich na świecie. Publikacja zawiera zaobserwowane taktyki, techniki i procedury (TTP), wskaźniki kompromitacji (IOC) oraz zalecenia mające na celu zmniejszenie zagrożenia związanego z zainfekowanymi *EdgeRouterami*. Atrybucja ataku wskazuje na Główny Zarząd Wywiadowczy Rosyjskiego Sztabu Generalnego (GRU), 85. Główne Centrum Służb Specjalnych (GTsSS), znane również jako APT28, *Fancy Bear* i *Forest Blizzard (Strontium)*, które wykorzystywały zainfekowane *EdgeRoutery* na całym świecie do zbierania danych uwierzytelniających, gromadzenia skrótów NTLMv2, proxy ruchu sieciowego oraz hostowania stron spearphishingowych w tym niestandardowych narzędzi. Warto dodać, że routery *Ubiquiti EdgeRouters* mają przyjazny dla użytkownika system operacyjny oparty na Linuksie, dzięki czemu są popularne zarówno wśród konsumentów, jak i cyberprzestępców. Routery te są często dostarczane z domyślnymi danymi uwierzytelniającymi i ograniczonymi lub zerowymi zabezpieczeniami zapory sieciowej w celu dostosowania do potrzeb dostawców bezprzewodowych usług internetowych (WISP). Ponadto routery nie aktualizują automatycznie oprogramowania, chyba że konsument skonfiguruje je w tym celu dlatego ten element również może stanowić główny słaby punkt tego typu urządzeń o czym każdy użytkownik powinien pamiętać.



Należy podkreślić, iż jednym ze współautorów publikacji jest Służba Kontrwywiadu Wojskowego, która jako jedyna polska instytucja wniosła wkład w opracowanie niniejszej publikacji. To kolejne działanie, które dowodzi skuteczności SKW w zakresie wykrywania i przeciwdziałania aktywności grup cyberszpiegowskich w cyberprzestrzeni.

Rekomendacje: Departament Sprawiedliwości Stanów Zjednoczonych, w tym FBI, oraz międzynarodowi partnerzy unieszkodliwili botnet GRU składający się z ww. routerów. Jednak właściciele takich urządzeń powinni podjąć również działania naprawcze opisane w publikacji, aby zapewnić długoterminowy sukces wspólnych wysiłków związanych z zakłóceniem oraz zidentyfikowaniem i naprawą wszelkich podobnych naruszeń bezpieczeństwa. Zalecane minimum to wykonać sprzętowy reset do ustawień fabrycznych, zaktualizować oprogramowanie sprzętowe do najnowszej wersji, zmienić domyślne nazwy użytkownika i hasła oraz wdrożyć strategiczne reguły zapory sieciowej na interfejsach po stronie WAN. Warto mieć te zalecenia na uwadze nie tylko jako właścicieli urządzeń Ubiquiti, ale także innych podobnych.

Link do publikacji: <https://www.ic3.gov/Media/News/2024/240227.pdf>



LolekHosted, Lockbit i Centralne Biuro Zwalczania Cyberprzestępczości w Operacji „CRONOS”

Funkcjonariusze Zarządu w Krakowie *Centralnego Biura Zwalczania Cyberprzestępczości* (CBZC) w 2023 roku zakończyli działalność nielegalnego hostingu typu bulletproof o nazwie „LolekHosted”.

Lolekhosted to firma hostingowa, która działała w Polsce i świadczyła usługi klientom z całego świata. *Bulletproof hosting* (znane również jako „cyberfortress hosting”) to forma usługi hostingowej, która charakteryzuje się odpornością na regulacje prawne oraz inne próby likwidacji działań nielegalnych lub nieetycznych witryn internetowych.

W ramach tej usługi udostępniano infrastrukturę sieciową cyberprzestępcom z całego świata. To oznaczało, że pomagali w prowadzeniu różnych nielegalnych działań, takich jak:

- Fikcyjne sklepy internetowe
- Phishing
- Reklamowanie fałszywych inwestycji
- Rozsyłanie spamu
- Ataki DDoS
- Dystrybucja złośliwego oprogramowania
- Fora o tematyce przestępczej

Funkcjonariusze Zarządu w Krakowie *Centralnego Biura Zwalczania Cyberprzestępczości* zatrzymali 5 członków zorganizowanej grupy przestępczej, w tym szefa grupy. Dwóch zatrzymanych trafiło do aresztu, a pozostali zostali zwolnieni za poręczeniem majątkowym.

Ofiarami przestępstw, które były popełniane z wykorzystaniem infrastruktury *LolekHosted* mogło paść setki tysięcy osób, firm i instytucji na całym świecie, a straty, jakie ponieśli, szacuje się na miliony dolarów.

Śledczy analizowali ogromne ilości danych, w tym ruch sieciowy i przepływy finansowe, które dokonywane były za pośrednictwem kryptowalut. Miało to na celu utrudnienie ustalenia przestępczego pochodzenia funduszy. Przeprowadzone czynności pozwoliły na wykrycie i namierzenie sprawców.

To ważny przykład walki z cyberprzestępczością, ale także pokazuje, jak istotne jest śledzenie i likwidacja tego rodzaju usług hostingowych, które ułatwiają działalność przestępczą w Internecie.

LockBit_57020AAC7997A933.exe	existing	exe	LBR_sparp.co.mx_57020AAC7997A933_1.07.22
LockBit_4BC59381BCBC5F6B.exe	existing	exe	LockBit_microtech.cn_30.05.22
Windows security.exe	existing	exe	LockBit_partners.nl_17.03.22
LockBit_gjan computers ltd_16.02.22 (2)	existing, already viewed		\Users\Administrator\Desktop\desktop2
LockBit_hpcserv.net_18.04.22 (1)	existing		\Users\Administrator\Desktop\desktop2
lockbit_indonesia_18.04.22.zip	existing	zip	\Users\Administrator\Downloads\r
LockBit_59063A21DCFF12FD.exe	existing	exe	\Users\Administrator\Downloads
lockbit_hpcserv.net_18.04.22.zip	existing	zip	\Users\Administrator\Downloads
lockbit_hungvuongco.com.vn_14.06.22.zip	existing	zip	\Users\Administrator\Downloads
lockbit_indonesia_18.04.22.zip	existing	zip	\Users\Administrator\Downloads
lockbit_microtech.cn_10.06.22.zip	existing	zip	\Users\Administrator\Downloads
lockbit_microtech.cn_30.05.22.zip	existing	zip	\Users\Administrator\Downloads
lockbit_partners.nl_17.03.22.zip	existing	zip	\Users\Administrator\Downloads



Gruntowna analiza zgromadzonych danych oraz kompleksowe rozpoznanie ukierunkowane na oprogramowania typu ransomware, pozwoliły na ustalenie kluczowych informacji związanych z oprogramowaniem szyfrującym *LockBit*. Na zabezpieczonych serwerach infrastruktury *LolekHosted* ujawniono pliki ściśle powiązane z ransomware *LockBit*:

```
~~~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak
site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner
your company will be safe.

Tor Browser Links:
http://lockbitapt2d73kr1bewgv27tquljgxr33xbwvwp6rkyieto7u4ncead.onion
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvpqkmevv4l3azl3gy6pyd.onion
http://lockbitapt34kvrp6xojy1ohhxrswvpzdffgs5z4pbbsywnzsbduqd.onion
http://lockbitapt5x4zkjbcqmz6frndhecqgagadevyiwqxukksnplidyvd7qd.onion
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4kykd.onion
http://lockbitapt72iw55njqnqymgsgsk5yp75ry7rirtdg4m7i42artsbqd.onion
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqqgpjpid.onion
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion
http://lockbitaptc2iq4atewz2ise62q63wfktyr14qtwtuk5qax262kgtzjqd.onion

Links for normal browser:
http://lockbitapt2d73kr1bewgv27tquljgxr33xbwvwp6rkyieto7u4ncead.onion.ly
http://lockbitapt2yfbt7lchxejug47kmqvqqxvvpqkmevv4l3azl3gy6pyd.onion.ly
http://lockbitapt34kvrp6xojy1ohhxrswvpzdffgs5z4pbbsywnzsbduqd.onion.ly
http://lockbitapt5x4zkjbcqmz6frndhecqgagadevyiwqxukksnplidyvd7qd.onion.ly
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4kykd.onion.ly
http://lockbitapt72iw55njqnqymgsgsk5yp75ry7rirtdg4m7i42artsbqd.onion.ly
http://lockbitaptawjl6udhpd323uehekiyatj6ftcxmkwe5sezs4fqqgpjpid.onion.ly
http://lockbitaptbdiajqtplcrigzgdjprwugkkut63nbvy2d5r4w2agyekqd.onion.ly
http://lockbitaptc2iq4atewz2ise62q63wfktyr14qtwtuk5qax262kgtzjqd.onion.ly

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically
motivated group and we want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data.
After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system
administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest
services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you a
decryptor or delete your data after you pay, no one will pay us in the future. You can get more information about us on Elon Musk's Twitter
https://twitter.com/hashtag/lockbit?f=live

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID

Download and install Tor Browser https://www.torproject.org/
Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID for correspondence with us that
no one will know about, tell it in the chat, we will generate a secret chat for you and give you his ID via private one-time memos service,
no one can find out this ID but you. Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we
attack hundreds of companies around the world.

Tor Browser personal link available only to you (available during a ddos attack):
http://lockbitsupqfyacidr6upt6nhhyipujvaablubuevxj6xy3frthvr3yd.onion
```

LockBit 3.0, znany również jako *LockBit Black*, to rodzina ransomware, która działała przez okres czterech lat. W tym czasie ataki wykorzystujące ich oprogramowanie były rozległe. *LockBit* zaatakował tysiące ofiar na całym świecie. Skutki tych ataków to straty sięgające miliardów funtów, dolarów i euro. Obejmują one zarówno płatności za okupy, jak i koszty związane z odzyskiwaniem danych. Grupa dostarczała usługę ransomware-as-a-service globalnej sieci hakerów, dostarczając im narzędzi i infrastruktury do przeprowadzania ataków. Kiedy sieć ofiary była zainfekowana złośliwym oprogramowaniem *LockBit*, dane były kradzione, a systemy szyfrowane. Ofiary były zmuszane do zapłaty okupu w kryptowalutach, aby zdekodować swoje pliki i zapobiec ujawnieniu ich danych.

Zebrane przez śledczych z Zarządu w Krakowie CBZC materiały w ramach prowadzonej współpracy zostały przekazane do *EC3 Europolu*. Komórka *EC3 (European Cyber Crime Centre)* to specjalistyczna jednostka zajmująca się zwalczaniem cyberprzestępczości, która wspiera państwa członkowskie Unii Europejskiej w zapobieganiu wszelkim formom poważnej przestępczości międzynarodowej i zorganizowanej, w tym cyberprzestępczości i terroryzmu. Wnikliwe analizy prowadzone przez wyspecjalizowanych analityków kryminalnych *EC3*



w ścisłej współpracy z funkcjonariuszami z Krakowa wykazały powiązania przedmiotowo-podmiotowe ze sprawami prowadzonymi w innych krajach. Po auspicjami *Europolu* została powołana nieformalna grupa śledczych działająca pod oznaczeniem kodowym *Cronos* zajmująca się przedmiotowym zagadnieniem. Wykorzystanie zaawansowanych metod pracy operacyjnej oraz złożona analiza przepływów kryptowalutowych pozwoliły ustalić tożsamość osoby narodowości rosyjskiej, która w 2023 roku uzyskała również obywatelstwo polskie. Okazało się, że ta osoba jest powiązana z badanym środowiskiem. Zaawansowana analiza przepływu kryptowalut wykazała, że na portfele należące do wspomnianej osoby dokonywane były zarówno bezpośrednie, jak i pośrednie wpłaty, pochodzące z klastra przypisanego sprawcom ataków oprogramowaniem *LockBit*. Należy wspomnieć, iż do tej pory przez zidentyfikowane portfele należące do zatrzymanego na terytorium Polski przetransferowano łącznie ponad 17,5 mln PLN.

W lutym 2024 roku w ramach międzynarodowej operacji „*Cronos*” została zamknięta strona internetowa grupy cyberprzestępczej *LockBit*, zablokowano ponad 200 adresów kryptowalutowych wykorzystywanych przez wspomnianą grupę oraz skonfiskowano 34 serwery. W operacji *Cronos* przeprowadzonej przez brytyjskie *National Crime Agency* (NCA), we współpracy z organami ścigania z całego świata tym z wyspecjalizowanymi w zwalczaniu cyberprzestępczości jednostkami *Żandarmerii Francuskiej C3N* oraz Polskiego CBZC, towarzyszyło zatrzymanie dwóch mężczyzn w Polsce i na Ukrainie. Dzięki współpracy służb cyberprzestępcy, przeciwko którym wniesiono akt oskarżenia w Stanach Zjednoczonych, zostali zatrzymani w Polsce i na Ukrainie, a przed sądem staną we Francji. Wspomniane zatrzymania członków grupy *LockBit* były możliwe dzięki zaawansowanym analizom oraz zinfiltrowaniu infrastruktury cyberprzestępców przez organy ścigania. Dodatkowo, dzięki pracy śledczych z *Europolu* na stronie www.nomoreransom.org opublikowano dekryptor, który umożliwia odszyfrowanie danych zaszyfrowanych przez oprogramowanie ransomware *LockBit 3.0*.

W międzynarodowej sprawie związanej z *LockBit* współpraca pomiędzy różnymi organami ścigania była kluczowym elementem sukcesu. Działania CBZC, *Prokuratury Krajowej*, *Europolu*, *EuroJustu* oraz Francuskiego *C3N* stanowią doskonały przykład, jak skuteczna i ważna jest współpraca na arenie międzynarodowej. Wspólnie działania agencji przyczyniły się do zamknięcia infrastruktury *LockBit* i zatrzymania osób podejrzanych. To ważny krok w walce z cyberprzestępczością, ale również przypomnienie, jak istotna jest międzynarodowa współpraca w zwalczaniu przestępczości w skali globalnej.



Cyberpodsumowanie miesiąca z perspektywy CSIRT KNF – Ochrona klienta

W lutym 2024 roku CSIRT KNF wykrył i zgłosił do zablokowania 6 345 domen (w styczniu 3 603 domeny), które wcześniej zakwalifikowane zostały jako wyłudzające dane (loginy i hasła do bankowości elektronicznej, informacje o kartach płatniczych, kody BLIK i/lub dane osobowe, etc.).

Podobnie jak pisaliśmy w minionych miesiącach, również w lutym 2024 trwał scenariusz znany pod nazwą „fraud inwestycyjny”. To metoda, w której przestępcy podszywają się pod znane osoby lub instytucje, celem nakłonienia potencjalnej ofiary do zainwestowania środków i otrzymania wysokiej stopy zwrotu. W rzeczywistości prowadzą grę psychologiczną, mającą na celu narażanie ofiary na wysokie starty finansowe. Nadal przestępcy wykorzystują technologie deepfake do tworzenia oszukańczych treści. Znane są także coraz częściej przypadki, w których przestępcy publikują reklamy informując o rzekomej możliwości odzyskania pieniędzy, które wcześniej zostały skradzione przez „nieuczciwego brokera”. W rzeczywistości wyłudniają środki finansowe od osób, które już wcześniej zostały przez nich oszukane (na podstawowy scenariusz, o możliwości inwestycji). W związku z tym, że na opisany wyżej scenariusz nadal daje się nabrać duża liczba osób oraz tracą oni wysokie kwoty to w minionym miesiącu UKNF opublikował kampanię informacyjno – ostrzegawczą nt. opisanego wyżej scenariusza przestępczego. Zachęcamy do zapoznania się z przygotowywanymi materiałami oraz przekazania ich rodzinie i znajomym:

https://www.knf.gov.pl/dla_konsumenta/kampanie_informacyjne/cyberoszustwa_inwestycyjne

CO ROBIMY > Kampanie > Cyberoszustwa inwestycyjne

Udostępnij Drukuj

Kampanie

Cyberoszustwa inwestycyjne



Schematy oszustw

Gdzie uzyskam pomoc?

Słownik

Materiały kampanii

Cyberoszuści wymyślają nowe sposoby, by ich działania były skuteczne. Ich celem jest pozyskanie danych, na przykład loginów i haseł do bankowości elektronicznej czy danych kart płatniczych, oraz nakłonienie osoby, którą chcą oszukać do wykonywania przelewów na należące do nich rachunki. Schematy swoich działań oszuści dostosowują do aktualnych trendów oraz sytuacji panującej w kraju i na świecie. Oszuści tworzą nowe scenariusze ataków, a także modyfikują te, którymi posługiwali się wcześniej. Jednak u podstaw każdej takiej kampanii, czyli akcji cyberoszustów, leży ten sam cel - wyłudzenie środków finansowych.

Co zrobić, żeby nie dać się oszukać?

Jednym z ważniejszych czynników jest umiejętność rozpoznania, że mamy do czynienia z oszustwem. Dlatego przygotowaliśmy kampanię edukacyjną Cyberoszustwa inwestycyjne. Omawiamy w niej scenariusze działań, w których cyberoszuści oferując rzekome możliwości wysokich zysków, przy jednoczesnym niskim ryzyku starty, manipulują daną osobą. Potrafią wyłudzać od niej środki finansowe nawet przez kilka miesięcy.

Z kampanii dowiesz się:

- ✓ jak rozpoznać fałszywą reklamę,
- ✓ jakie przykładowe sposoby wykorzystują oszuści prowadząc grę psychologiczną,
- ✓ jak ustrzec się przed działaniami oszustów.

To co jeszcze wydarzyło się w lutym 2024, to m.in:



- fałszywe wiadomości e-mail oraz oszukańcze reklamy na platformie Facebook podszywające się pod polskie banki,
- podszywanie pod Ministerstwo Finansów i opublikowana przez przestępców informacja o rzekomej możliwości otrzymania odszkodowania,
- podszywanie pod Fundację im. Stefana Batorego i fałszywa zbiórka pieniędzy na pomoc Ukrainie,
- wykorzystanie wizerunku Meta i e-mailowa dystrybucja kampanii phishingowej, której celem były osoby wykupujące reklamy na platformie Facebook oraz Instagram, w wiadomościach znajdowała się informacja o rzekomych problemach z kontem reklamowym, potrzebie weryfikacji danych osobowych lub koniecznością zapłaty za usługi reklamowe

Powyższe scenariusze miały na celu wyłudzenie danych uwierzytelniających do bankowości elektronicznej oraz informacji o kartach płatniczych, a na dalszy etapie wyprowadzenie pieniędzy z rachunku ofiary.

W lutym 2024 roku przestępcy podszywając się pod polskie banki, starali się również infekować urządzenia klientów. Przy współpracy z zespołem CERT Orange Polska, zidentyfikowaliśmy złośliwą aplikację mobilną infekującą urządzenia z systemem Android. Po zainstalowaniu jej na urządzeniu, starała się pozyskać szereg uprawnień m.in.:

- dostęp do sieci Wi-Fi, lokalizacji, kamery oraz mikrofonu,
- odczytywanie wiadomości,
- pobieranie ostatnich 10 SMSów.

Aplikacja prawdopodobnie podstawiała fałszywą stronę logowania w momencie otwierania legalnej aplikacji, w ten sposób przestępcy mogli pozyskać poświadczenia logowania, a następnie wykradając wiadomości tekstowe, znajdowali kody SMS.

Jedną z metod ochrony przed wymienionymi wyżej i innymi działaniami cyberprzestępców jest wiedza. Dlatego (jak zawsze) zachęcamy do śledzenia informacji o bieżących schematach i scenariuszach przestępczych na naszych profilach w mediach społecznościowych:

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. 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: cert.pl