BNB Chain został wstrzymany z powodu ataku hakerskiego. Hakerzy wykradli ponad 100 mln dolarów

Wczoraj, tj. 6 października 2022 BNB Chain został wstrzymany z powodu ataku hakerskiego. Atakującym, którzy wykorzystali exploit na tzw. „moście międzyłańcuchowym” (ang. *cross-chain bridge)*, udało się wykraść tokeny Binance Coin (BNB) o wartości ponad 100 mln dolarów.

Początkowo osoby odpowiedzialne za prowadzenie sieci BNB Chain czasowo wstrzymały jej działanie, tłumacząc się „podejrzaną, nieregularną aktywnością”, a na oficjalnym koncie na Twitterze pojawiła się informacja o „potencjalnym nadużyciu” i „konserwacji” sieci, w wyniku których wstrzymano wszystkie wpłaty i wypłaty. **Teraz wiadomo jednak, że chodziło o skuteczny atak hakerski i wykorzystanie wspomnianego exploita.**

O ataku oraz wstrzymaniu Binance Smart Chain (BSC) informował także na swoim Twitterze popularny CEO giełdy Binance, Changpeng Zhao (CZ):

Zgodnie z wstępnymi, pierwszymi szacunkami, z sieci Binance Smart Chain wyprowadzono fundusze o wartości oscylującej w granicach 70-80 mln dolarów. Obecnie szacuje się jednak, **że**

łupem hakerów padło ok. 100 mln dolarów – co stanowi równowartość jednej czwartej ostatniego spalania tokenów BNB (*BNB Burn).*

Zobacz też: rok 2023 rokiem Binance Coina?

CEO Binance przyznał także, że sam spał w momencie ataku i docenił wysiłki zespołu oraz społeczności, które doprowadziły do szybkiego wstrzymania działania sieci. Dodał także, że programiści potrzebują czasu by w pełni zrozumieć główne przyczyny problemu oraz oszacować wielkość strat, dlatego odradza pośpiech. Dzięki działaniom wspomnianych programistów oraz społeczności, udało się już zamrozić ok. 7 mln dolarów ze skradzionych 100.

BNB Chain wstrzymany – cena tokena Binance Coin (BNB) reaguje spadkiem o prawie 4%

Wiadomość o ataku i wyprowadzeniu środków doprowadziła do spadku kursu tokena najpopularniejszej giełdy na świecie o ok. 3,7%.

Źródło: CoinMarketCap

Pomimo bardzo poważnej sytuacji, zarówno deweloperzy

odpowiedzialni za BNB Chain jak i CEO giełdy Binance, Changpeng Zhao zapewniają, że wszystkie środki posiadaczy tokena BNB są bezpieczne i nienarażone na stratę.

Źródło

Śmiertelna pułapka internetu czyha na dzieci. Pornografia. Uzależnienie. Cyber-przemoc. Gry śmierci. Uwodzenie.

Sidła zastawione! Śmiertelna pułapka internetu czyha na dzieci. Pornografia. Uzależnienie. Cyber-przemoc. Gry śmierci. Uwodzenie.

Dzieci, które nie umieją jeszcze bezpiecznie korzystać z internetu, mogą wpaść w śmiertelną pułapkę.

Bardzo aktualnym przykładem jest tu tragedia 12-letniego Archiego Battersbee, który stał się ofiarą igrania ze śmiercią podczas tzw. internetowego wyzwania, zwanego „Blackout Challenge" (w polskim tłumaczeniu „utrata przytomności"). Do tej pory ta demoniczna zabawa kosztowała życie już siedmioro dzieci. A to nie jedyny „wilczy dół", do którego mogą wpaść nasze pociechy, kiedy bez żadnej kontroli,

swobodnie serfują w sieci.

7 kwietnia 2022 roku rodzice znaleźli Archiego w stanie nieprzytomności. Leżał, bez oznak życia, na podłodze w rodzinnym domu. Zabrano go do szpitala, gdzie lekarze stwierdzili, iż mózg nastolatka uległ bardzo poważnym uszkodzeniom wskutek niedotlenienia. Dziecko podłączono do aparatury podtrzymującej życie. Po jakimś czasie dyrekcja szpitala podjęła decyzję o odłączeniu Archiego od tej aparatury, gdyż zdaniem lekarzy **pień mózgu umarł i chłopca nie da się uratować.** Rodzice nie zgadzali się z decyzją szpitala. Podali sprawę do sądu, który rację przyznał jednak lekarzom. Archiego 7 sierpnia odłączono od aparatury, niedługo po tym przestał oddychać.

Rozpoczęło się dochodzenie jak doszło do tej tragedii. Ostatecznie ustalono, że nastolatek dał się namówić do udziału w tzw. „wyzwaniu", upowszechnionym na portalu społecznościowym Tik Tok. Wyzwanie to, zwane z angielska „Blackout Challenge" (utrata przytomności) polega na możliwie najdłuższym wstrzymaniu oddechu. Wówczas to w mózgu pozbawionym tlenu powstają halucynacje, podobne do wizji narkotycznych. Kiedy jednak człowiek zbyt długo nie oddycha, wówczas najpierw traci przytomność, a potem umiera.

Do tej pory, na całym świecie, ujawniono co najmniej 7 przypadków zgonów dzieci, które „bawiły się" w „Blackout Challenge". Ich rodzice złożyli pozwy do sądów przeciwko platformie Tik Tok, oskarżając ją o nie zablokowanie śmiercionośnego challengu. Szefowie Tik Tok bronią się podając, iż zablokowano możliwość wyszukiwania hasła Blackout. Gracze znaleźli jednak tzw. „obejście". Wyzwanie „utrata przytomności" nie jest bynajmniej pierwszym takim igraniem ze śmiercią za pośrednictwem internetu. Wcześniejsze grupowe „wyciskanie" adrenaliny w mediach społecznościowych, też miało tragiczne skutki.

Uzależnienie

Internet jest pełen pułapek i sideł zastawionych na dzieci, nieświadomych czyhających tam na nie niebezpieczeństw. Samo długotrwałe przebywanie w odrealnionym, cyfrowym świecie prowadzi do uzależnienia. Dziecko uzależnione od internetu, traci kontakt z rzeczywistością, a kiedy pozbawi się go dostępu do sieci, staje się agresywne. Czasem tak bardzo, iż potrafi zranić, albo nawet zabić. Świeża jest tragedia, do której doszło w tym roku, w domu położonym niedaleko hiszpańskiego miasteczka Elche. Kiedy rodzice, z powodu złych wyników w nauce, odcięli dostęp do internetu swojemu 15-letniemu synowi, ten wpadł w szał i zastrzelił całą swoją rodzinę – rodziców i brata.

Skala problemu uzależnienia od bycia w sieci widoczna jest chociażby bo gwałtownie rosnącej liczbie psychiatrycznych oddziałów odwykowych od interentu na całym świecie, również w Polsce. Ministerstwo zdrowia uruchomiło niedawno program „Terapia dla dzieci i młodzieży uzależnionych od nowych technologii cyfrowych”. Już 12 dużych ośrodków zdrowia psychicznego w całej Polsce bierze udział w tym programie. Ośrodki te znajdują się na ogół w dużych miastach, takich jak m.in. Warszawa, Wrocław, Białystok, Szczecin, Łódź, Toruń czy Siemianowice Śląskie.

Pornografia

Jednym z największych niebezpieczeństw grożących dzieciom, poruszających się w sieci, jest wszechobecna tam pornografia, która bardzo mocno degeneruje młode umysły i szybko je uzależnia. Według badań naukowych mózg dziecka nie jest przygotowany na zmierzenie się z treściami pornograficznymi, które czynią w nim wielkie spustoszenie. Te przedwczesne i nieuporządkowane doznania seksualne, mają bardzo negatywny wpływ na późniejsze – życie dorosłe. – *Osoby, które miały wczesny kontakt z pornografią, np. w wieku 12 lat bądź*

wcześniej, o wiele częściej wskazują na problemy związane z czerpaniem satysfakcji w związku małżeńskim – powiedział podczas jednego z wykładów wybitny specjalista – dr hab. Piotr Rzymski z Zakładu Medycyny Środowiskowej na Uniwersytecie Medycznym w Poznaniu. Niestety te problemy są częstym powodem rozbicia małżeństwa. Z danych statystycznych wynika również, że osoby uzależnione od pornografii o wiele częściej, niż osoby nie uzależnione, dopuszczają się gwałtów i przemocy wobec kobiet.

Rozwiązaniem dla rodziców są na pewno odpowiednie programy, które blokują strony pornograficzne oraz tego rodzaju reklamy. Jedną z najskuteczniejszych takich zapór są przeglądarki internetowe, produkowane przez firmy profesjonalnie zajmujące się tworzeniem programów antywirusowych. Pomysłowość naszych dzieci jest jednak ogromna i potrafią one skutecznie poradzić sobie z różnego rodzaju blokadami stron, dlatego nieodzowna jest rodzicielska kontrola. Co jakiś czas trzeba zasiąść do komputera naszej pociechy i sprawdzić czy wszystko jest w porządku, bo bez tego zdrowego monitoringu, nasza pociecha może stać się dla nas ciężkim utrapieniem. Wystarczy, że same naturalne przemiany rozwojowe w wieku nastoletnim są dla rodziców poważnym wyzwaniem, po co więc sobie jeszcze dokładać. Pewien mądry i wesoły człowiek powiedział „Kto przeżyje trudy wieku nastoletniego swoich dzieci – temu czyściec będzie darowany”. I tej nadziei się trzymajmy.

Gry śmierci

Inną „toksyną” związaną z komputerem, grasująca nie tylko w przestrzeni internetu, są agresywne gry komputerowe. Pełno w nich przemocy, krwawych i brutalnych scen. Oglądnie, a do tego jeszcze uczestnictwo w zabijaniu na ekranie, wulgarny język gier, nie może pozostać bez negatywnego wpływu na umysły graczy. Cyfrowe gry są coraz bardziej nasycone wszelkiego rodzaju dewiacjami i agresją. Ich bohaterowie to przeważnie seryjni mordercy, psychopaci, zombi, wampiry i demony.

Godziny, które gracze spędzają w takim ciemnym towarzystwie, na pewno im nie służą. Jak mówi stare, mądre przysłowie „Z kim przestajesz takim się stajesz”.

Kiedy któregoś razu odwiedzałem kuzyna, wszedłem do pokoju jego nastoletnich synów, żeby się z nimi przywitać. Obaj grali właśnie na komputerze w bardzo drastyczną grę. Gdy zobaczyłem na ekranie monitora skalę okrucieństwa i przemocy, aż zimny pot mnie oblał. Poczułem się jakbym znalazł się nagle w przedsionku piekła. Zapytałem chłopaków jak mogą na to patrzeć i to wiele godzin. Jeden z nich odpowiedział ze spokojem „To tylko gra”. Jak muszą być znieczulone sumienia osób uczestniczących w tych cyfrowych igrzyskach śmierci? Jak stępiona ludzka wrażliwość?

Uwodzenie

Dla pedofilów sieć internetowa stała się siecią, którą łowią dzieci. Te szatańskie łowy doczekały się nawet swojej anglojęzycznej nazwy – grooming. Pedofil tworzy profil na ulubionym portalu społecznościowym upatrzonej ofiary. Podaje się tam za dziecko, najlepiej rówieśnika osoby małoletniej, którą chce skrzywdzić. Zwyrodnialec obserwuje ofiarę, stara się zdobyć jej zaufanie poprzez przyjazne rozmowy, wysyłanie swoich fałszywych zdjęć. Wszystko to, aby wyłudzić od dziecka jego adres zamieszkania lub szkoły. Kiedy mu się to uda, wówczas może już uderzyć.

Cyberprzemoc

Agresja w internecie przejawia się na wiele sposobów i ma wiele imion. Trollowanie to różnego typu nieprzyjazne zachowania wobec innych użytkowników portali społecznościowych, prowadzone w celu rozbicia ich dyskusji. Flamingiem nazywa się sprowadzanie rozmowy do tonu jak najbardziej agresywnego i wulgarnego. Doskonale znany hejt to obraźliwe, nienawistne wypowiedzi kierowane wobec innych osób.

Można by tu jeszcze długo wymieniać te angielskie imiona nienawiści, obecnej w sieci. Ale może lepiej sobie tego oszczędźmy. Dość powiedzieć, że przemoc w internecie nie jest wirtualna, ale realna. Do tego stopnia, że potrafi zabić.

Mój przyjaciel, opowiedział mi historię dziewczyny o bardzo kruchej psychice, która po zawodzie miłosnym, targnęła się na swoje życie. Odratowano ją. Przeszła terapię, stanęła na nogi. Zdawało się, że poukłada sobie życie. Niestety internetowi hejterzy przypuścili na nią atak. Jeden z tych nienawistników napisał „jest nieudacznikiem, nawet samobójstwa nie potrafi popełnić”. To było jak kamieniowanie. Policja podała w komunikacie, że druga próba samobójcza była niestety skuteczna. Ale tak naprawdę to nie ona się zabiła – zabiła ją ludzka nienawiść, zwana internetowym hejtem.

Nie pozostawiajmy dzieci samych z cyfrową hydrą

Najnowsze badania wskazują, że współczesny rodzic jest bardzo często nieobecny w cyber świecie swojego dziecka. W 60 proc. domów rodzice nie stawiają dzieciom żadnych granic w korzystaniu z internetu, a wiadomo, że dzieci same sobie tych granic nie postawią. Siedzą, czy leżą godzinami ze wzrokiem utkwionym w ekran monitora lub smartfona. Trwanie w takim bezruchu jest częstym powodem nadwagi, lub innej skrajności – niedowagi, gdyż dziecko urzeczone wirtualną rzeczywistością, nie da rady oderwać się od niej, nawet na posiłek. Brak ruchu, świeżego powietrza prowadzi do utraty zdrowia, osłabienia odporności. Wady wzroku to obecnie wśród dzieci i młodzieży prawdziwa plaga, a to też efekt obciążania wzroku gapieniem się w ekran z bliskiej odległości. Kolejnym „efektem ubocznym” braku ograniczania przez rodziców czasu, które dzieci spędzają przy monitorach, jest brak snu naszych pociech. Niewyspanie odbija się niezdrowa czkawką w postaci braku zdolności koncentracji, co prowadzi do słabych wyników w nauce i

wzmożonej nerwowości, a nawet depresji i nerwic.

Warto więc znaleźć czas dla dziecka. Nie wykręcać się sianem, że muszę dużo pracować, zarabiać, mam inne obowiązki. Jeżeli nie znajdziemy czasu dla dziecka, to możemy je – stracić. Cóż wówczas będą znaczyły nasze pieniądze, praca i obowiązki? Przecież czas przeżyty z osobą bliską, to czas najlepiej przeżyty. Postarajmy się więc wyrwać swoje dziecko, choć na krótki czas, ze świata wirtualnego i zainteresować go światem realnym, który jest bez porównania piękniejszy i ciekawszy. Mogą w tym pomóc wspólne spacery, sporty, gry, zabawy na świeżym powietrzu, w otoczeniu przyrody. Dobrze jest też pomóc dziecku w odkrywaniu jego talentów i zachęcić, aby je rozwijało. Wspólne, dobre spędzanie czasu razem z dzieckiem buduje zdrową relację, która jest podstawą, do tego, aby dziecko nie bało się nam powiedzieć o swoich problemach i radościach, również do tego, aby wysłuchało naszej opowieści o Stwórcy, świecie i prawdziwym sensie życia.

Adam Białous

Wielu przypuszcza, że cyberataki nie mogą zabijać ludzi. To nieprawda

Cyberataków nie należy lekceważyć i traktować jako niewinnej

zabawy młodych ludzi. To poważne przestępstwa, które mogą prowadzić również do śmierci.

- Grupa ekspertów ostrzega, że □□Korea Północna mogłaby wykorzystać techniki groźnych cyberataków.
- Cyberprzestępcy mogą na przykład przejąć kontrolę nad oczyszczalnią wody i zmienić mieszankę chemiczną, aby była toksyczna…
- …albo przeniknąć do systemów komputerowych elektrowni jądrowej, powodując poważne awarie.

Koreański dziennikarz Jung Min-ho pisze:

> *Jednym z najbardziej niedocenianych zagrożeń bezpieczeństwa pochodzących z Korei Północnej są jej możliwości cyberataków. Wielu przypuszcza, że □□hakerzy nie mogą zabijać ludzi. Ale mogą.*

Cyberprzestępcy mogą przejąć kontrolę nad oczyszczalnią wody i zmienić mieszankę chemiczną, aby była toksyczna, lub mogą przeniknąć do systemów komputerowych elektrowni jądrowej, powodując poważne awarie. W ostatnich latach w wielu częściach świata podejmowano próby takich cyberataków, niektóre z nich zakończyły się pośrednio śmiercią lub obrażeniami.

Grupa ekspertów ostrzega, że □□Korea Północna mogłaby wykorzystać takie techniki, gdyby wybuchła wojna na Półwyspie Koreańskim, w raporcie RAND Corporation zatytułowanym "Charakterystyka zagrożeń związanych z północnokoreańską bronią chemiczną i biologiczną, impulsem elektromagnetycznym i zagrożeniami cybernetycznymi".

Choi Kang, prezes Asan Institute for Policy Studies i jeden ze współautorów wspólnego raportu napisanego z think tankiem RAND Corporation, powiedział na konferencji prasowej w instytucie w Seulu we wtorek.

> *Infrastruktura w Korei Południowej wydaje się być bardzo*

> *podatna na cyberataki Północy. Widzieliśmy kilka przypadków w systemach bankowych… Ale co z inną infrastrukturą, taką jak zaopatrzenie w wodę lub elektryczność? To spowodowałoby chaos.*

Możliwe scenariusze

Jednym z możliwych scenariuszy może być wykolejenie pociągów załadowanych śmiercionośnymi chemikaliami. Inne możliwe cele obejmują tamy, szpitale, lotniska i sieci energetyczne, których wiele systemów komputerowych zostało już wcześniej przenikniętych przez Koreę Północną.

Raport mówi, że domniemane rozmieszczenie wirusa Stuxnet przez Stany Zjednoczone i Izrael w celu uszkodzenia irańskich wirówek do wzbogacania nuklearnego oraz rosyjski program złośliwego oprogramowania towarzyszący inwazji na Ukrainę w tym roku mogą służyć jako przykłady do naśladowania i rozwijania przez Koreę Północną.

Źródło

Polscy hakerzy związani z Anonymous zapowiadają publikację kilkuset polskich firm powiązanych z Rosją

Grupa Squad303 (nazwa odnosi się do historycznego Dywizjonu 303 biorącego udział w Bitwie o Anglię), która należy do znanej siatki Anonymous, zapowiedziała publikację listy nawet kilkuset polskich firm powiązanych z Rosją.

Polscy hakerzy już od początku wojny są zaangażowani w ujawnianie prawdy na temat prawdziwych działań Federacji Rosyjskiej na Ukrainie.

> *– Od maja pracujemy nad kolejnym projektem, którego celem jest ujawnienie WSZYSTKICH firm powiązanych z Rosjanami w Europie. W tej chwili mamy bazę imion, nazwisk, adresów, odpowiedników PESEL i NIP, nazw firm i rodzaju powiazań z nimi obywateli Rosji (udziałowiec/akcjonariusz/członek organu) w UK, Danii, Polsce i kilku innych krajach w Europie. Krok po kroku, kraj po kraju będziemy ujawniali posiadane dane – możemy przeczytać w mailu wysłanym przez hakerów do redakcji „Głosu Wielkopolskiego”.*
>
> *– To bardzo pracochłonne zajęcie, więc projekt będzie trwał jeszcze kilka miesięcy, ale dane z Polski postaramy się ujawnić już w sierpniu. Dlaczego o tym pisze? Bo w tych bazach jest bardzo wiele nazwisk (np. w UK 14 660 rekordów), a my nie mamy zasobów, żeby zbudować pełen obraz powiazań personalno-biznesowych. To już rola opinii publicznej, a w szczególności mediów – wyjaśniają przedstawiciele grupy, którzy zapowiadają publikację listy firm działających w Polsce w ciągu najbliższych 2-3 tygodni, czyli w drugiej połowie sierpnia.*

Niestety pomimo wielu pakietów sankcji ze strony Unii

Europejskiej rosyjscy oligarchowie potrafili skutecznie ochronić się przed nieprzyjemnymi konsekwencjami. Najlepszy przykład stanowi jeden z najbogatszych Rosjan i dobry znajomy Władimira Putina, czyli Aleksiej Mordaszow, którego majątek na ten moment wycenia się na 29 mld dol. Ten biznesmen już kilka lat temu trafił na amerykańską „listę Putina", a w warunkach wojny, kiedy Federacja Rosyjska napadła na Ukrainę, musiał szybko działać, by chronić swoje aktywa.

Miliarder co prawda stracił luksusowy jacht oraz rezydencję we Włoszech, jednak tego samego nie można powiedzieć o jego firmach. W tym miejscu, jak wskazują media, ważne okazały się nie tylko kontakty w Moskwie, ale i w Berlinie. Parę miesięcy temu agencja Reutera informowała o tym, jak Mordaszow zdołał uniknąć zamrożenia ponad miliarda funtów w akcjach niemieckiego koncernu turystycznego TUI AG, odsprzedając niemal wszystkie swoje udziały spółce Ondero Limited z Brytyjskich Wysp Dziewiczych – tę kontroluje jego żona Marina Mordaszowa.

Chociaż Ministerstwo Gospodarki Niemiec uruchomiło w tej sprawie śledztwo, to trudno spodziewać się szybkich działań i wielkich sankcji, a zwłaszcza że jeszcze na początku 2021 z powodu koronawirusa niemiecki rząd wsparł firmę TUI AG kwotą 1,25 miliarda euro. To nie jedyny taki manewr w wykonaniu Aleksieja Mordaszowa. Serwis Bloomberg na początku marca donosił, że oligarcha przekazał też swojej żonie kontrolę nad pakietem akcji brytyjskiej spółki górniczej Nordgold o wartości ok. 1,1 mld dol.

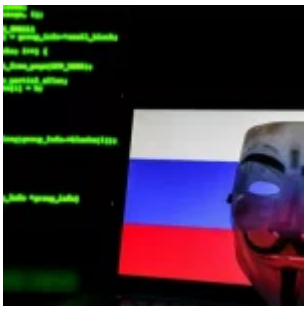
W naszym kraju TUI Group prowadzi działalność jako spółka TUI Poland. Według statystyk jest to największe biuro turystyczne, które przed wybuchem pandemii zajmowało 40 procent rynku. Firma nie została objęta sankcjami przez polskie władze właśnie ze względu na zmiany prawne, których dokonał Mordaszow. Niemniej jednak głównym akcjonariuszem spółki wciąż pozostaje rosyjski oligarcha. Poza tym można zadać pytanie, czy prywatne dane Polaków mogą być bezpieczne w teoretycznie

niemieckim, a w praktyce rosyjskim koncernie.

Być może hakerzy z Anonymous ujawnią więcej tego typu powiązań w wykonaniu rosyjskich oligarchów, którzy robią wszystko, aby ukryć swoje wpływy w firmach działających w Europie.

Źródło

Anonymous włamali się do kolejnego rosyjskiego banku. 800 GB danych



Anonymous poinformowało, że udało im się włamać do bazy danych banku kraju-agresora Rosji. Zagrozili wyciekiem do sieci 800 GB poufnych informacji.

Stało się to znane z anonimowej wiadomości na portalu społecznościowym Twitter . Został opublikowany w poniedziałek 18 kwietnia.

Mówimy o Społecznym Banku Handlowym w Petersburgu – PSCB. Klientami tej instytucji finansowej są rosyjscy oligarchowie.

https://twitter.com/Anonymous_Link/status/1516116675078377474?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1516116675078377474%7Ctwgr%5E%7Ctwcon%5Es1

„Anonymous złamał inny rosyjski bank. Planujemy uwolnić 800 GB poufnych danych! Zespół hakerów podpisujących papiery wartościowe Anonymous złamał rosyjski bank JSC Bank PSKB, z którego korzystają oligarchowie” – podał portal społecznościowy.

W przeddzień okazało się, że Anonymous złamał jedną z firm Gazpromu . Hakerzy umieścili w Internecie 768 000 listów od pracowników Gazprom Linde Engineering, które są częścią rosyjskiego giganta gazowego. Firma specjalizuje się w projektowaniu obiektów dla rafinerii ropy naftowej.

Ponadto otrzymali dostęp do 700 GB danych rządu rosyjskiego. Anonymous przejął także kontrolę nad systemem monitoringu Kremla i pokazał pierwszy materiał filmowy z wnętrza.

Światowe Forum Ekonomiczne naciska na Wielki Reset poprzez „cyberatak o cechach podobnych do COVID”

Światowe Forum Ekonomiczne (WEF) to międzynarodowa organizacja pozarządowa rzekomo poświęcona ulepszaniu świata poprzez biznes, politykę i środowisko akademickie. Ostatnio zagłębia się w świat cyberbezpieczeństwa. W rzeczywistości WEF dąży do

Wielkiego Resetu za pomocą „ cyberataku o cechach podobnych do COVID”.

WEF odegrał wiodącą rolę w plandemii COVID-19. Naciskało na paszporty szczepionkowe, cyfrowe śledzenie kodów kreskowych i, co najważniejsze, Wielki Reset. Teraz ostrzega świat przed możliwym cyberatakiem obejmującym cały świat, który może sparaliżować globalny system finansowy.

WEF przygotowuje ludzi do oczekiwania cyberataku obejmującego cały świat

Na początku 2021 r. WEF Center for Cybersecurity ogłosiło Cyber □□Polygon 2021. To internetowa konferencja poświęcona cyberbezpieczeństwu. Tegoroczny Cyber □□Polygon ma jeden cel: dowiedzieć się, jak wygląda „cyberatak z cechami podobnymi do COVID”.

We wcześniejszych wersjach WEF powiedziało, że Cyber □□Polygon 2021 skupi się na oprogramowaniu ransomware, podatności globalnego łańcucha dostaw na cyberataki i waluty cyfrowe. WEF obiecało również przeprowadzenie „ćwiczeń szkoleniowych na żywo”, które są odpowiedzią na „ukierunkowany atak łańcucha dostaw na ekosystem korporacyjny w prawdziwym życiu”.

„Wszyscy wiemy, ale wciąż nie zwracamy na niego wystarczającej uwagi, przerażający scenariusz kompleksowego cyberataku, który całkowicie wstrzymałby dostawy energii, transport, usługi szpitalne, nasze społeczeństwo jako całość” – powiedział Klaus Schwab, założyciel i prezes wykonawczy WEF. „Kryzys COVID-19 byłby pod tym względem postrzegany jako niewielkie zakłócenie w porównaniu z poważnym cyberatakiem”.

Schwab dodał, że ważne jest, aby WEF wykorzystał trwającą pandemię COVID-19, aby „przemyśleć lekcje społeczności cyberbezpieczeństwa, aby wyciągnąć i poprawić naszą nieprzygotowanie na potencjalną cyberpandemię”.

Schwab wygłosił te komentarze w zeszłym roku, pokazując, że

WEF od pewnego czasu planuje przygotowywać ludzi do Wielkiego Resetu wywołanego cyberatakiem. 9 lipca, w dniu rozpoczęcia konferencji Cyber Polygon, Schwab powtórzył swoje sianie strachu, przypominając ludziom o ostatnich cyberatakach, które miały miejsce.

„W ciągu ostatnich kilku miesięcy widzieliśmy na przykład ataki ransomware wymierzone w szpitale, infrastrukturę krytyczną, systemy szkolne, sieć energetyczną i wiele innych podstawowych usług" – powiedział.

„Ataki ransomware są złożone, a przedsiębiorstwa przestępcze zwiększają swoją skalę i wpływ. Podkreśla to potrzebę ustrukturyzowanego wielostronnego, wielostronnego podejścia do zabezpieczenia naszego społeczeństwa przed nimi".

Trwają ogólnoświatowe ćwiczenia WEF w zakresie cyberpandemii

Ćwiczenie szkoleniowe Cyber Polygon składa się z ponad 200 zespołów z 48 krajów. Firmy takie jak IBM, Santander i Ernst and Young wysłały swoje zespoły ds. bezpieczeństwa cybernetycznego, aby wziąć udział w tym ogólnoświatowym ćwiczeniu.

„Nieuniknione jest, że pewnego dnia dojdzie do większego ataku", powiedział John Sancenito, prezes firmy konsultingowej ds. bezpieczeństwa z siedzibą w Pensylwanii. „To, o czym mówi się dzisiaj i w ciągu najbliższych kilku dni, jest potencjalną sytuacją w świecie rzeczywistym".

Sancenito jest zainteresowane tematem tegorocznego ćwiczenia na żywo. Jeśli cyberatak wycelowany jest w łańcuch dostaw w Stanach Zjednoczonych, może wpłynąć na codzienne życie ludzi poprzez zamknięcie infrastruktury krytycznej, takiej jak sieć energetyczna lub oczyszczalnie ścieków.

„Co byś zrobił, gdybyś nie mógł uzyskać dostępu do swoich kont bankowych, Internetu lub nagle przestał działać telefon

komórkowy? Są to rzeczy, które ludzie naprawdę muszą przemyśleć, ponieważ pewnego dnia możemy stanąć w obliczu takiego kryzysu” – powiedział Sancenito.

Ćwiczenie na żywo Cyber Polygon trwa kilka dni. W chwili obecnej trwa nadal.

Artykuł przetłumaczono z: newstarget.com

Zadbaj o silne hasła do kont. Zniwelujesz zagrożenie cyberatakiem i ochronisz swoje dane, pieniądze

W cyberprzestrzeni coraz częściej przechowujemy wiele cennych informacji – prywatnych i nie tylko. Od nas zależy, czy odpowiednio je zabezpieczymy. Wydział Promocji Polityki Cyfrowej Kancelarii Prezesa Rady Ministrów (KPRM) przypomina, że internetowi przestępcy atakują nie tylko duże przedsiębiorstwa, lecz także zwykłych ludzi. Eksperci namawiają do stosowania silnych haseł do kont bankowych, poczty elektronicznej, na portalach społecznościowych, a także w telefonie czy w komputerze, by nikt ich nie przejął, nie ukradł tożsamości, nie pozbawił oszczędności bądź nie miał dostępu do naszych prywatnych danych. Jak zatem powinniśmy

tworzyć kody zabezpieczające?

Mankamenty haseł

Cyfryzacja KPRM podaje, że część cyberataków uderza właśnie w hasła użytkowników, dlatego należy wystrzegać się najpowszechniejszych błędów, a więc unikać prostych haseł i nie używać tego samego kodu zabezpieczającego do różnych kont. Wskazane jest tworzenie unikatowych haseł dla każdej witryny.

Jakich jeszcze błędów nie powinniśmy popełniać? Nie zabezpieczajmy dostępu do swoich danych najpopularniejszymi hasłami lub oczywistymi wyrażeniami, typu: „hasło”, „123456”, „qwerty”, „piłka nożna”, „wpuscmnie”, ani imieniem własnym bądź kogoś z bliskiego otoczenia, bądź ulubionego zwierzaka. Ta sama zasada dotyczy też danych osobowych, które łatwo zdobyć, takich jak: data urodzenia, numer telefonu, numer rejestracyjny samochodu, nazwa ulicy, numer mieszkania lub domu.

Niewskazane jest stosowanie wyrażeń identycznych z nazwą użytkownika, lub nawet jej częścią, oraz sekwencji kolejnych liter, liczb lub innych znaków, np. „abcde”, „12345”, „QWERTY”, jak również dwóch lub trzech kolejno powtarzających się ciągów znaków, np. „bbbb2bbb”.

Ponadto odradza się używanie pojedynczego wyrazu dowolnego języka, pisanego normalnie lub wspak, nie wystarczy też, że poprzedzimy lub zakończymy go znakiem specjalnym lub cyfrą.

W komunikacie zwrócono uwagę, by przy zmianie hasła do istniejącego konta nie użyć tego samego sformułowania, co poprzednio lub po niewielkiej modyfikacji, np. zmiana z „hasło1” na „hasło2”.

Cyberklucz

Cyfryzacja KPRM przypomina: „Hasła są jak klucze do sejfu lub domu”. Trzeba dbać, żeby nie dostały się w niepowołane ręce.

Dlatego radzi, aby tworzyć dłuższe hasła, składające się z 12 lub 14 znaków, które będą zawierały co najmniej jeden znak z każdej z następujących grup: małe litery, duże litery, liczby, znaki specjalne.

Konstruując unikatowe hasło, można, jak podpowiadają specjaliści, wykorzystać frazy, wybrać np. łatwy do zapamiętania cytat z piosenki i użyć pierwszych liter poszczególnych słów. Poleca się zastępowanie liter bądź wyrazów liczbami i symbolami.

Podano przykłady: „Mam dwadzieścia lat” można zamienić na M@m2dzie$ciAl4T, a „Mam psa” na M@m%p$@.

Można stosować też metodę łączenia trzech losowych słów, np. „kawatramwajryba”, byleby nie były zbyt proste do odgadnięcia.

Podkreślono, że zabezpieczeń nie powinno się zapisywać na papierze, przesyłać np. w mailu albo wpisywać haseł, gdy ktoś to widzi, bo nawet bardzo silne kody mogą w takich przypadkach okazać się bezużyteczne.

Cyfryzacja KPRM ostrzega przed podszywającymi się np. pod pracowników pomocy technicznej hakerami, którzy próbują wyłudzić dane użytkownika i hasła. Jak zaznaczono: „Wiarygodne witryny i organizacje nigdy nie poproszą o nazwę użytkownika i hasło w wiadomości e-mail lub przez telefon”.

Hasło powinniśmy bezzwłocznie zmienić, jeśli doszło do jego naruszenia lub nawet jeśli tylko przypuszczamy, że ktoś mógł je wykraść.

Nie należy również wpisywać hasła, gdy korzystamy z cudzego komputera.

Aby dane były bezpieczniejsze, potrzebne jest nie tylko silne hasło, lecz także stosowanie dwuetapowej weryfikacji.

Dodatkowe informacje o zabezpieczaniu danych w cyberprzestrzeni można znaleźć w poradniku „Jak chronić się przed cyberatakami”.

Źródła: PAP, Cyfryzacja KPRM.

Wyciekły dokumenty: KPCh wykorzystała płatnych trolli do przeciwdziałania wiadomościom o epidemii pomoru świń w Internecie

Seria wewnętrznych dokumentów chińskich władz cenzurujących ujawniła, w jaki sposób trolle internetowe są wykorzystywane aby manipulować opinią publiczną na korzyść chińskiego reżimu.

Zapisy z miejskiego oddziału Luoyang Administracji Cyberprzestrzeni – głównej chińskiej agencji cenzury internetowej – pokazują, że władze wynajęły internetowe trolle do pisania postów w mediach społecznościowych wychwalających władze. Dokumenty wyciekły przez zaufane źródło.

Tym trollom zapłacono 11 juanów (około 1,62 $) za każdy post, który napisali.

Manipulacja opinią publiczną

Luoyang to miasto położone w prowincji Henan w środkowych Chinach.

W połowie lutego 2019 r. Wokół firmy Sanquan Food z siedzibą w Henan wybuchł skandal dotyczący bezpieczeństwa żywności. Stwierdzono, że pierogi tej marki zawierają ślady wirusa wywołującego afrykański pomór świń (ASF).

ASF po raz pierwszy wybuchł wśród populacji świń w Chinach w sierpniu 2018 roku i szybko rozprzestrzenił się po całym kraju. ASF jest śmiertelny dla świń i wieprzy, ale nie ma wpływu na ludzi. Zwierzęta hodowlane są zwykle poddawane ubojowi, aby zapobiec rozprzestrzenianiu się choroby.

Wielu chińskich rolników używa ludzkich odchodów jako nawozu. Jeśli taki nawóz zawiera aktywne wirusy ASF, może zanieczyścić źródła wody i potencjalnie przenosić chorobę na więcej świń.

Informacje o skażonych pierogach szybko rozprzestrzeniły się na chińskich platformach społecznościowych, zmuszając władze do publicznego przyznania się do incydentu.

16 lutego 2019 r. wszystkie internetowe i fizyczne sklepy spożywcze w kraju zdjęły pierogi Sanquan z półek.

Administracja Luoyang Cyberspace zgłosiła władzom miasta, jak wynajęte trolle internetowe próbowały manipulować opinią publiczną po skandalu żywnościowym w Sanquan.

Jeden troll z internetowym pseudonimem „Qingqi Suoyou" napisał: „Od czasu pierwszej [na świecie] epidemii ASF około sto lat temu, żaden człowiek nie został zarażony wirusem ASF. Tak więc wirus ASF nie wpłynie na produkty wieprzowe. Możesz jeść mięso i produkty z nim związane".

Zrzut ekranu z komentarzem opublikowanym przez wynajętego trolla, mającym na celu przeciwdziałanie negatywnym wiadomościom o produktach wieprzowych chińskiej firmy spożywczej zawierającej wirusa afrykańskiego pomoru świń.
Inny wynajęty troll o imieniu „Ruguo” napisał: „Wirus ASF zostanie zabity w wysokich temperaturach. Możesz jeść [pierogi], gotując je w całości.”

Inni próbowali bagatelizować wiadomości jako plotki. Wynajęty troll o internetowej nazwie „Qinghe” napisał: „Nie wierz w plotki i nie rozpowszechniaj ich. Wszystkie duże przedsiębiorstwa mogą prześledzić źródło użytych surowców”.

Niektórzy próbowali wykorzystać okazję, by chwalić władze.

Troll „Kantaiyang” napisał: „Nasz kraj zawsze traktuje bezpieczeństwo żywności jako coś bardzo ważnego. Wierzę, że rząd udzieli naszym ludziom odpowiedzi [o źródle wirusa]”.

„Hai’ai” napisał: „Nie możemy wątpić, że chińska Państwowa Administracja ds. Żywności i Leków oraz Sanquan Food są proaktywne w obliczu problemu. Najważniejsze jest rozwiązanie problemu. Nie powinniśmy wszystkiego kwestionować, a spokojnie czekać”.

USA oskarża 6 rosyjskich oficerów GRU o globalną operację hakerską

Departament Sprawiedliwości oskarżył sześciu rosyjskich hakerów wojskowych o angażowanie się w serię ataków na infrastrukturę, wybory czy biznesy innych krajów, co zostało opisane jako „najbardziej uciążliwa i destrukcyjna serii ataków komputerowych przypisana do jednej grupy."

Oskarżeni, będący agentami rosyjskiej agencji wywiadu wojskowego, znanej jako GRU, rzekomo stosowali różne taktyki cybernetyczne, w tym rozmieszczanie destrukcyjnego szkodliwego oprogramowania w celu wspierania interesów rządu rosyjskiego w destabilizacji i ingerowaniu w systemy polityczne i gospodarcze innych krajów, powiedział Departament Sprawiedliwości (DOJ).

GRU to ta sama agencja, która rzekomo była zaangażowana w próby włamania się, aby ingerować w wybory prezydenckie w USA w 2016 roku.

Wśród celów znajduje się ukraińska sieć elektroenergetyczna, Ministerstwo Finansów i Służba Skarbu Państwa; Partia polityczna prezydenta Francji Emmanuela Macrona i francuscy politycy; gospodarze, uczestnicy, partnerzy, uczestnicy i systemy informatyczne Zimowych Igrzysk Olimpijskich w PyeongChang 2018; organizacje i podmioty badające zatrucie środkiem nerwowym Siergieja Skripala; Gruzińskie firmy i

jednostki rządowe; oraz firmy i placówki medyczne w Stanach Zjednoczonych.

„Żaden kraj nie wykorzystał swoich zdolności cybernetycznych tak złośliwie i nieodpowiedzialnie jak Rosja, bezmyślnie powodując bezprecedensowe szkody w celu osiągnięcia niewielkiej przewagi taktycznej i zaspokojenia napadów złośliwości" – powiedział zastępca prokuratora generalnego ds. Bezpieczeństwa narodowego John C. Demers podczas konferencji prasowej 19 października ogłaszając zarzuty.

Zgodnie z aktem oskarżenia hakerzy wdrożyli „jedne z najbardziej destrukcyjnych dotychczas szkodliwych programów na świecie" – takie jak KillDisk, Industroyer i NotPetya – które spowodowały rozległe szkody, w tym przerwy w dostawie energii na Ukrainie i zakłócenia pracy tysięcy komputerów używanych do obsługi programu Winter 2018 Igrzyska Olimpijskie.

Mężczyźni zostali oskarżeni o spisek mający na celu dokonywanie oszustw i nadużyć komputerowych, spisek w celu popełnienia oszustwa elektronicznego, oszustwa elektronicznego, niszczenia chronionych komputerów i kradzieży tożsamości. Każdy jest oskarżony w każdym przypadku w akcie oskarżenia zwróconym przez federalne trybunały sądowe w Pittsburghu.

Plakat przedstawiający sześciu poszukiwanych oficerów rosyjskiego wywiadu wojskowego.
(Departament sprawiedliwości)

Departament powiedział, że kilku mężczyzn zostało wcześniej oskarżonych o ich role w rzekomym ingerowaniu w wybory w USA w 2016 roku.

Demers powiedział, że zarzuty powinny być dowodem na to, że Stany Zjednoczone nie powinny zaakceptować oferty prezydenta Władimira Putina dotyczącej cyber „resetu” między dwoma krajami. Porozumienie wymagałoby od obu zapewnienia gwarancji, że nie będą angażować się w „cyberwtrącanie się” do swoich wyborów.

> *„Rosja z pewnością ma rację, że zaawansowane technologicznie narody, które aspirują do przywództwa, mają szczególną odpowiedzialność za zabezpieczenie światowego porządku i przyczynianie się do powszechnie akceptowanych norm, pokoju i stabilności. To właśnie robimy tutaj dzisiaj”- powiedział Demers.*

> *„Ale ten akt oskarżenia obnaża wykorzystanie przez Rosję jej zdolności cybernetycznych do destabilizacji i ingerowania w wewnętrzne systemy polityczne i gospodarcze innych krajów, stanowiąc w ten sposób zimne przypomnienie, dlaczego jej propozycja jest niczym innym jak nieuczciwą retoryką oraz cyniczną i tanią propagandą”.*

Departament Sprawiedliwości powiedział, że ataki spowodowały prawie miliard dolarów strat trzech ofiar w USA, w tym Heritage Valley Health System w Pensylwanii. Mężczyźni rzekomo wdrożyli złośliwe oprogramowanie NotPetya, które spowodowało „niedostępność list pacjentów, historii pacjentów, plików badań i danych laboratoryjnych”.

„Heritage Valley utraciło dostęp do swoich krytycznych systemów komputerowych (takich jak te związane z kardiologią, medycyną nuklearną, radiologią i chirurgią) na około tydzień, a administracyjne systemy komputerowe na prawie miesiąc, powodując tym samym zagrożenie dla zdrowia i bezpieczeństwa publicznego,” zgodnie z oświadczeniem wydziału.

Inne cele w USA to TNT Express BV, spółka zależna FedEx Corp., oraz duży producent farmaceutyczny.

Źródło:

theepochtimes.com