Chiny twierdzą, że grupa cyberprzestępcza Volt Typhoon jest aktywem CIA wymyślonym w celu ich zdyskredytowania

Organizacja cyberprzestępcza Volt Typhoon trafiła na pierwsze strony gazet za swoje ataki w ostatnich latach i często donosi się, że ścigają ją amerykańskie władze. Chińskie Narodowe Centrum Reagowania na Wirusy Komputerowe (CVERC) twierdzi jednak, że Volt Typhoon został w rzeczywistości stworzony przez Stany Zjednoczone i ich sojuszników z NATO w celu zniszczenia ich reputacji i właśnie opublikowali trzecią część trwającej serii, która ich zdaniem potwierdza ich twierdzenia.

Oskarżyli oni Stany Zjednoczone, Kanadę, Wielką Brytanię, Australię i Nową Zelandię, wraz z licznymi agencjami wywiadowczymi, o angażowanie się w cyberszpiegostwo przeciwko Chinom i innym krajom, w tym Japonii, Niemcom i Francji, a także użytkownikom Internetu na całym świecie.

Następnie oskarżyli Stany Zjednoczone o rozpoczęcie operacji fałszywej flagi mających na celu ukrycie cyberataków. Chiny twierdzą, że Ameryka robi to wszystko, aby stworzyć iluzję „tak zwanego zagrożenia chińskimi cyberatakami”.

FBI, Agencja Bezpieczeństwa Cybernetycznego i Infrastruktury (CISA) oraz NSA obwiniają grupę Volt Typhoon o atakowanie krytycznej amerykańskiej infrastruktury.

CVERC opublikowało trzecią część swojej serii w formie dokumentu w wielu językach zatytułowanego „Lie to Me: Volt Typhoon III – Unravelling Cyberespionage and Disinformation Operations Conducted by US Government Agencies”. Przedstawiono w nim swoje twierdzenia, opierając się na poprzednich raportach o tym, jak władze amerykańskie wykonują „bezpodstawne uprawnienia do szpiegowania wszystkich ludzi na całym świecie, w tym Amerykanów za pośrednictwem sekcji 702 FISA, aby agencje rządowe USA mogły wyeliminować zagranicznych konkurentów i bronić cybernetycznej hegemonii i długoterminowych interesów monopoli”.

Według raportu, Chiny współpracowały z dziesiątkami ekspertów ds. cyberbezpieczeństwa, aby dojść do wniosku, że USA i Microsoft nie mogą udowodnić, że Chiny były zaangażowane w Volt Typhoon; raport nie wymienia ekspertów, z którymi się konsultowano.

Raport wskazuje również na programy takie jak gromadzenie danych PRISM i Biuro Operacji Dostosowanego Dostępu NSA, z których oba zostały ujawnione przez Edwarda Snowdena i mają podobne zdolności do tych z Volt Typhoon.

W raporcie powtórzono również wiele materiałów wymienionych w pierwszych dwóch częściach serii, w tym znane amerykańskie programy, takie jak sekcja 702 dotycząca bezprawnej inwigilacji cudzoziemców oraz struktura Marble, której CIA używa do cyberoperacji, która została wcześniej ujawniona przez Wikileaks.

Złośliwe oprogramowanie Volt Typhoon przeniknęło do krytycznej amerykańskiej infrastruktury

Złośliwe oprogramowanie Volt Typhoon było wykorzystywane do infiltracji krytycznych amerykańskich systemów i

infrastruktury, zagrażając fizycznemu bezpieczeństwu Amerykanów poprzez atakowanie systemów energetycznych, kontroli ruchu lotniczego i portowego, kolejowych i wodnych.

Wyciekłe dokumenty, które pojawiły się na początku tego roku, wskazywały również na udział CCP w złożonej zagranicznej kampanii cyberszpiegowskiej, która wywołała szereg ostrzeżeń ze strony ekspertów ds. cyberbezpieczeństwa. Celem programu jest destabilizacja wrogów i zapewnienie Chinom lepszej pozycji do przygotowania się do potencjalnej wojny z USA i ich sojusznikami.

Dokumenty wykazały, że chińska grupa znana jako I-Soon infiltrowała departamenty rządowe w Korei Południowej, Wietnamie, Tajlandii, Indiach i organizacjach stowarzyszonych z NATO.

Poprzez Volt Typhoon KPCh stara się zapewnić sobie przewagę militarną nad USA za pomocą środków niemilitarnych.

Casey Fleming, dyrektor generalny firmy doradczej BlackOps Partners, powiedział The Epoch Times: „KPCh jest hiper-koncentrowana na osłabianiu USA pod każdym kątem, aby wygrać wojnę bez walki. Tak właśnie wygląda III wojna światowa. To szybkość technologii, skrytość nieograniczonej wojny i brak zasad”.

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

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

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