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”.