CHINY UZYSKAŁY DOSTĘP DO INFRASTRUKTURY PRZEMYSŁU OBRONNEGO USA

Hakerzy powiązani z Chinami wykorzystali luki w zabezpieczeniach oprogramowania VPN w celu uzyskania dostępu do sieci i systemów podmiotów z sektora obronnego, rządowego i finansowego z całego świata, w tym przede wszystkim Stanów Zjednoczonych. Wrogie działania są przejawem cyberszpiegostwa. Pekin stanowczo odpiera zarzuty, nazywając je „nieodpowiedzialnymi i opartymi na złych intencjach".

Co najmniej dwie grupy hakerskie powiązane z Chinami wykorzystały w ostatnich miesiącach luki w popularnym oprogramowaniu VPN (ang. virtual private networking) firmy Pulse Secure do prowadzenia wrogich działań. Produkt jest używany zarówno przez podmioty prywatne, jak i państwowe, w tym rządy.

W oficjalnym oświadczeniu specjaliści Pulse Secure wskazali, że w wyniku podatności „ograniczona liczba klientów" doświadczyła incydentów bezpieczeństwa w swoich sieciach. Jak podkreślili, po identyfikacji problemu firma od razu rozpoczęła współpracę z „czołowymi ekspertami", w tym m.in. FireEye, CISA oraz Stroz Friedberg, aby zneutralizować zagrożenie.

Pulse Secure stwierdziło, że konkretnie chodzi o trzy luki w zabezpieczeniach ich produktu, z którymi był już wcześniej problem (CVE-2019-11510, CVE-2020-8243 i CVE-2020 -8260) oraz jedną podatnością, jaką dopiero wykryto (CVE-2021-22893). Jak deklaruje firma, w aktualizacji, której wydanie zaplanowano na początek maja, ma zostać uwzględniona poprawka podnosząca bezpieczeństwo. Równocześnie zalecono klientom zmianę haseł w celu zmniejszenia ryzyka.

Zdaniem firmy zajmującej się cyberbezpieczeństwem FireEye luki były wykorzystywane przez co najmniej dwie grupy hakerskie związane z Chinami – jedna z nich miała działać na zlecenie rządu ChRL, przy czym druga realizować inicjatywy Pekinu. Co na to wskazuje? Charles Carmakal, wiceprezes Mandiant, powiedział w rozmowie z agencją Reutera, że zgodnie z oceną analityków firmy sposób działania hakerów, metody, narzędzia i taktyka są charakterystyczne dla Chin.

Zdaniem specjalistów celem wrogich działań były podmioty z sektora obronnego, rządowego i finansowego na całym świecie. Jednak hakerzy wykazywali szczególne zainteresowanie amerykańskim przemysłem obronnym.

Eksperci Mandiant obecnie śledzą 12 rodzin złośliwego oprogramowania związanych z wykorzystaniem urządzeń połączonych z Pulse Secure VPN.

Państwo Środka stanowczo zaprzecza twierdzeniom FireEye, wskazując, że są one „nieodpowiedzialne i oparte na złych intencjach" – przytacza stanowisko Pekinu agencja Reutera. Jak dodano, Chiny sprzeciwiają się jakimkolwiek rodzajom cyberataków i podejmują kroki w celu ich zwalczania.

Wagę problemu podkreśla również wydanie specjalnego alertu bezpieczeństwa przez amerykańską Agencję ds. Cyberbezpieczeństwa i Infrastruktury (CISA). Stwierdzono w nim, że cyberataki wykorzystujące luki w produkcie Pulse Secure „mają wpływ na agencje rządowe USA, podmioty odpowiedzialne za infrastrukturę krytyczną oraz firmy z sektora prywatnego”.

CISA ostrzega, że wykorzystanie wskazanych podatności przez hakerów umożliwia im obejście uwierzytelniania, w tym wieloskładnikowego, a także kradzież informacji, takich jak np. dane logowania.

W tym miejscu warto pamiętać, że Chiny zostały uznane przez społeczność wywiadowczą USA za jedno z głównych zagrożeń dla bezpieczeństwa narodowego Stanów Zjednoczonych. Jak informowaliśmy w naszym materiale, w opublikowanym raporcie „Annual Threat Assessment of the US Intelligence Community” podkreślono, że Państwo Środka w coraz większym stopniu łączy rosnącą siłę militarną z ekonomicznymi, technologicznymi i dyplomatycznymi możliwościami w celu realizacji własnych interesów, gdzie jednym z nich jest osłabienie pozycji USA na arenie międzynarodowej.

Amerykański wywiad jednoznacznie stwierdził, że Pekin ucieka się do szpiegostwa oraz kradzieży, co ma zwiększyć jego możliwości technologiczne. „Oceniamy, że Chiny stanowią zagrożenie cyberszpiegowskie oraz posiadają znaczne cybermożliwości (…) Chińskie działania w cyberprzestrzeni zwiększają ryzyko cyberatków na Stany Zjednoczone” – wskazano w raporcie. Amerykańskie służby nie mają wątpliwości, że Chiny będą prowadzić cyberataki, które mogą przyczynić się do zakłócenia działania infrastruktury krytycznej Stanów Zjednoczonych.

Czytaj też: Wywiad USA o źródłach (cyber)zagrożeń dla Stanów Zjednoczonych. Nie tylko Rosja i Chiny