aut. Szymon Palczewski 01.04.2020

CYBERATAKI WYMIERZONE W OCHRONĘ ZDROWIA. FBI ODKRYWA TAJEMNICE GLOBALNEJ KAMPANII

FBI wykryło złośliwą kampanię hakerską, w ramach której cyberprzestępcy prowadzili zaawansowane operacje wymierzone w wrażliwe branże, takie jak ochrona zdrowia. Specjaliści wskazują, że incydenty miały charakter globalny.

FBI poinformowało o wykryciu działalności hakerów, którzy wykorzystywali trojana Kwampir Remote Access (RAT) do prowadzenia złośliwych, szeroko zakrojonych operacji cyberprzestępczych – czytamy w oficjalnym komunikacie FBI.

Biuro wskazuje, że Kwampirs RAT to modułowy wirus RAT, który uzyskuje dostęp do systemów komputerów i innych urządzeń w celu przejęcia kontroli nad wewnętrznymi sieciami ofiary. „Dzięki analizom kryminalistycznym FBI zidentyfikowało branże, takie jak opieka zdrowotna, sektor energetyczny w Stanach Zjednoczonych, Europie, Azji i na Bliskim Wschodzie, które są obiektem zainteresowania hakerów" – stwierdzono w komunikacie.

Specjaliści FBI podkreślają, że operacje z wykorzystaniem Kwampira były prowadzone przeciwko między innymi podmiotom opieki zdrowotnej. Odznaczały się one wysokim poziomem skuteczności przez co cyberprzestępcy uzyskali szeroki i trwały dostęp do sieci wybranych celów. „Docelowe podmioty obejmują zarówno duże międzynarodowe firmy opieki zdrowotnej, jak i lokalne organizacje szpitalne" – wyjaśnia FBI.

Zakres złośliwych działań był różnorodny. Hakerzy infekowali zarówno konkretne urządzenia medyczne, jak i bardziej złożone i zaawansowane układy. Kampanie z użyciem trojana Kwampirs, według danych FBI, trwają od co najmniej 2016 roku.

Eksperci oceniają, że hakerzy uzyskali dostęp do dużej liczby szpitali z całego świata poprzez łańcuch dostaw dedykowanego oprogramowania oraz sprzętu medycznego. Zgodnie z przedstawionymi danymi, cyberprzestępcy posługujący się wirusem Kwampira z powodzeniem zyskali, a następnie utrzymywali stałą obecność w sieciach ofiar przez okres od trzech do 36 miesięcy.

FBI wyszczególniło również szereg rekomendacji dotyczących poprawy poziomu cyberbezpieczeństwa w celu lepszej ochrony przez złośliwymi operacjami hakerskimi. Wśród nich można wskazać między innymi na regularne aktualizowanie aplikacji oraz systemu operacyjnego, aby w ten sposób zlikwidować ewentualne luki w zabezpieczeniach. Bardzo ważne jest również prowadzenie cyklicznego monitoringu i skanowania systemu oraz wrażliwych plików w celu identyfikowania nieprawidłowości oraz błędów, co pozwoli ustalić obszary zwiększonego ryzyka.

Czytaj też: FBI: zlikwidowano rosyjską platformę przeznaczoną do nielegalnego obrotu danymi