Prokuratorzy nie chcą, by FBI wyłączyło serwery

26 lutego 2012

Prokuratorzy federalni zwrócili się do sądu z wnioskiem, by nakazał FBI przedłużenie pracy serwerów zastępujących DNSChangera o kolejne 4 miesiące. Serwery mogłyby zostać wyłączone dopiero 9 lipca.

DNSChanger zainfekował około 4 milionów komputerów na całym świecie. Zmienia on konfigurację DNS zarażonych maszyn tak, by łączyły się one z serwerami cyberprzestępców, na których wyświetlane są reklamy. FBI zlikwidowało botnet DNSChanger w listopadzie ubiegłego roku i po uzyskaniu zezwolenia sądu podstawiło zań swoje własne serwery, gdyż bez nich zarażone komputery straciłyby dostęp do internetu. Biuro planuje wyłączenie serwerów 8 marca. Ci użytkownicy, a znajdują się wśród nich osoby indywidualne, firmy oraz instytucje rządowe, którzy nie wyczyścili swoich komputerów z DNSChangera nie będą mogli połączyć się z siecią. Prokuratorzy domagają się jednak, by FBI dało internautom więcej czasu na działanie.

Tymczasem FBI stara się o ekstradycję sześciu Estończyków, którym zarzuca rozpowszechnianie szkodliwego kodu. Cała szóstka została zatrzymana w październiku, w ramach prowadzonego od dwóch lat śledztwa o kryptonimie Operation Ghost Click. FBI podejrzewa, że twórcy DNSChangera zarobili 14 milionów dolarów na przekierowywaniu użytkowników na witryny z reklamami.

Szkodliwy kod kierował użytkowników do wybranych przez nich witryn poprzez serwery przestępców. Uniemożliwia on tez pobranie poprawek oraz wyłącza oprogramowanie antywirusowe.

Prokuratorzy domagający się od FBI dłuższego utrzymywania serwerów zdają sobie najwyraźniej sprawę z faktu, że użytkownicy nie spieszą się z usuwaniem DNSChangera ze swoich

komputerów. Przeprowadzone dwa tygodnie temu badania wykazały, że co najmniej 250 z 500 największych firm świata wciąż posiada co najmniej 1 komputer zarażony tym szkodliwym kodem.

Opracowanie: Mariusz Błoński
Na podstawie: SC Magazine
Źródło: Kopalnia Wiedzy