FBI odetnie część internautów od sieci?

4 lutego 2012

Specjaliści ostrzegają, że 8 marca część użytkowników internetu mogą czekać poważne kłopoty. Właśnie na ten dzień FBI zapowiedziało wyłączenie swoich serwerów, które zastąpiły serwery przestępców, kierujących użytkowników na złośliwe witryny.

W listopadzie FBI zlikwidowało botnet DNSChanger. Jego twórcy infekowali komputery i manipulowali adresami internetowymi tak, że użytkownicy trafiali na witryny, których jedynym celem było wyświetlanie reklam. FBI zastąpiło serwery przestępców własnymi maszynami, dzięki czemu komputery zainfekowane przez botnet mogły bez przeszkód łączyć się z internetem. Ponadto FBI było w stanie zidentyfikować zarażone maszyny.

Jednak Biuro z góry założyło, że zastępcze serwery będą działały tylko przez jakiś czas, by użytkownicy komputerów zarażonych DNSChangerem mieli czas na wyczyszczenie komputerów ze szkodliwego kodu. „Zastępcza sieć" FBI ma zostać wyłączona właśnie 8 marca. Oznacza to, że komputery, które nadal są zarażone, stracą dostęp do internetu, gdyż będą usiłowały łączyć się z nieistniejącymi serwerami DNS.

Eksperci ostrzegają, że wiele komputerów wciąż nie zostało wyczyszczonych ze szkodliwego kodu. Z danych firmy ID wynika, że co najmniej 250 z 500 największych światowych firm oraz 27 z 55 największych amerykańskich instytucji rządowych używa co najmniej jednego komputera lub routera zarażonego DNSChangerem. Nieznana jest liczba indywidualnych użytkowników, którzy mogą mieć kłopoty.

Zespół odpowiedzialny w FBI za zwalczanie DNSChangera rozważa przedłużenie pracy serwerów. Jednak nawet jeśli nie zostaną one wyłączone 8 marca, to niewiele się zmieni. Internauci,

zarówno prywatni jak i instytucjonalni, nie dbają o to, co dzieje się z ich komputerami. Można tak wnioskować chociażby z faktu, że największa liczba skutecznych ataków jest przeprowadzonych na dziury, do których łaty istnieją od dawna, jednak właściciele komputerów ich nie zainstalowali. Przykładem takiej walki z wiatrakami może być historia robaka Conficker, który wciąż zaraża miliony maszyn, mimo, że FBI od 2009 roku prowadzi aktywne działania mające na celu oczyścić zeń internet.

Ponadto, jeśli FBI nie wyłączy swoich serwerów, to DNSChanger nadal będzie groźny. Robak uniemożliwia bowiem pobranie poprawek, co oznacza, że niektóre z zarażonych nim maszyn nie były aktualizowane od wielu miesięcy, a to wystawia je na jeszcze większe niebezpieczeństwo.

Firmy, które chcą sprawdzić, czy ich komputery zostały zarażone DNSChangerem powinny skontaktować się z witryną DNS Changer Working Group. Użytkownicy indywidualni mogą skorzystać z narzędzia do sprawdzenia komputera.

Opracowanie: Mariusz Błoński
Na podstawie: InfoWorld
Źródło: Kopalnia Wiedzy