Armia komputerów-zombie generujących Bitcoiny

10 kwietnia 2013

To nie sen nawiedzonego informatyka, który dowiedział się o wzrastającym kursie wirtualnej waluty, tylko realne zagrożenie, przed którym ostrzega Kaspersky Lab.

Porsche Cayman – kupiony przez jednego z internautów za Bitcoiny – pobudził wyobraźnię czytelników. Jak poinformował przedwczoraj CNET Australia, powołując się na analizę Dmitrija Bestużewa z Kaspersky Lab, za pośrednictwem Skype'a rozpowszechniany jest nowy koń trojański, którego zasadniczym celem jest nieuczciwe pozyskiwanie Bitcoinów.

Przypomnijmy w skrócie, jak działa sieć Bitcoin. Przede wszystkim jest to sieć peer-to-peer oparta na otwartoźródłowym oprogramowaniu. Dystrybucja nowo wygenerowanych bitmonet odbywa się szacunkowo sześć razy na godzinę w losowych odstępach czasu. Potencjalnie może je zgarnąć każdy użytkownik sieci – prawdopodobieństwo, że tak się stanie, zależy jednak od ilości udostępnianej przez niego mocy obliczeniowej.

Mamy więc prostą zależność: im więcej maszyn pracuje na rzecz danego użytkownika, tym większe ma on szanse na otrzymanie wirtualnej waluty. Zauważyli to także twórcy wspomnianego wyżej trojana (producenci antywirusów nadają mu różne nazwy). Atak wykryto 4 kwietnia, jego celem okazali się przede wszystkim mieszkańcy Włoch, Rosji, Polski, Kostaryki, Hiszpanii, Niemiec i Ukrainy.

– Atak nieprzypadkowo rozpoczął się w momencie, gdy kurs wymiany waluty Bitcoin osiągnął swoje apogeum. W dniu 5 kwietnia 1 moneta była warta 132 dolary – jest to ogromny wzrost w porównaniu z rokiem 2011, kiedy to 1 moneta była warta 2 dolary. Jest to zbyt kuszące, aby mogło zostać zignorowane przez cyberprzestępców – komentuje Siegiej Łożkin

z Kaspersky Lab.

Jak pisałam wcześniej, odnośnik do szkodliwego programu jest rozpowszechniany za pomocą Skype'a. Zwykle towarzyszy mu tekst „to moje ulubione zdjęcie z tobą" (lub podobny). Link oszuści skracają przy użyciu bit.ly, jego kliknięcie skutkuje rozpoczęciem pobierania pliku skype-img-04_04-2013.exe – już w tym momencie w głowie użytkownika powinna zapalić się czerwona lampka, bo .exe to plik wykonywalny, nie graficzny.

Najwyraźniej wielu tego nie wie, bo z obliczeń Kaspersky Lab wynika, że w dniu rozpoczęcia infekcji średnia liczba kliknięć złośliwego odsyłacza dochodziła do dwóch tysięcy na godzinę. Zainstalowanie się trojana w systemie oznacza przyłączenie go do botnetu pozyskującego Bitcoiny dla jego twórców.

Jak ustrzec się przed zarażeniem? Naczelna zasada brzmi: z rozwagą klikaj w linki docierające za pośrednictwem komunikatorów i innych usług online.

Autor: Anna Wasilewska-Śpioch
Na podstawie: CNET, Kaspersky Lab
Źródło: Dziennik Internautów