

Kryptograficzna waluta znów zawiodła

7 września 2012

Bitcoiny miały gwarantować bezpieczne i anonimowe przekazywanie pieniędzy. W praktyce kryptograficzna waluta ma jednak sporo wad, a kolejne problemy utrudniają jej zdobycie popularności.

Kolejna giełda padła ofiarą włamywaczy, którzy zdołali wykraść jej użytkownikom około 24 tysiące Bitcoin (po obecnym kursie około 800 tysięcy złotych). Szanse, że pieniądze powrócą do poszkodowanych, są obecnie bardzo niewielkie.

Bitcoiny to nic innego, jak jedna z walut, która powstała stosunkowo niedawno, bo zaledwie w 2009 roku. Całość została stworzona przez Satoshiego Nakamoto i jest jedną z pierwszych kryptowalut – konceptu opisanego już ponad 20 lat temu na jednej z list dyskusyjnych cyberpunków.

Walutę wyróżnia przede wszystkim to, że występuje wyłącznie w formie cyfrowej i każdy internauta posiadający komputer, może ją również dla siebie generować (potocznie „wykopywać”). Proces wydobywania nowych Bitcoin jest jednak bardzo powolny, więc nie ma co liczyć na szybkie wzbogacenie się.

Cyfrową walutę można przechowywać wyłącznie w... cyfrowych portfelach. Warto zauważyć, że budowa Bitcoina oparta o P2P pozwala na anonimowe posiadanie tego typu pieniędzy, a także ich transfer z ominięciem banków. Całość jest więc praktycznie niewykrywalna dla organizacji rządowych.

Anonimowość, bezpieczeństwo, wygoda (Bitcoiny można przenosić np. na pendrive), nie gwarantują jednak, że pieniądze tego typu nie można ukraść. Dobitnie przekonało się o tym w ostatnim czasie wielu użytkowników.

Właściciel giełdy Bitfloor, która umożliwia wymianę Bitcoin na znane waluty, jak euro czy dolary, poinformował na forum usługi o poważnym włamaniu. Choć oficjalnie prosił tylko o pomoc, w praktyce przyznał się jednak do istotnego zaniedbania – przechowywał kopię kluczy do cyfrowych portfeli w niezaszyfrowanej formie. Właśnie tego typu pliki dostały się w ręce przestępców.

– Wykorzystując klucze, włamywacze byli w stanie przesyłać Bitcoiny – napisał na forum właściciel Bitfloor. Szybko okazało się, że cyberprzestępcy zdołali przetransferować z kont użytkowników giełdy około 24 tysiące Bitcoin, wartych łącznie około 800 tysięcy złotych.

– Zarządzanie kluczami to w takim przypadku wyzwanie – przyznał w rozmowie z SecurityWeek Todd Thiemann z firmy Vormetric. – Jeśli szyfrujesz wiele lokalizacji i w grę wchodzi wiele kluczy szyfrujących, musisz opracować dobry sposób, by je przechowywać i nimi zarządzać.

Choć kurs Bitcoin wahał się znacznie w ostatnich latach, dzięki cyfrowym kantorom możliwe jest wymienianie ich na znane wszystkim waluty. Niestety są to jednak giełdy, które nazwać można co najwyżej „amatorskimi” i jak widać, często nie przestrzegającymi podstawowych zasad bezpieczeństwa.

Anonimowość transakcji w tym przypadku również może zadziałać na niekorzyść samych internautów. Włamywacze, którzy przetransferowali pieniądze z portfeli użytkowników giełdy, pozostają przecież niezidentyfikowani.

Opracowanie: Adrian Nowak

Na podstawie: BitcoinTalk, SecurityWeek

Źródło: [Dziennik Internautów](#)