Megint feltörték a feltörhetetlen pénztárcát

A Bitfi kihúzta a gyufát a hackereknél, a második alkalommal már kénytelen volt, hogy nem nevezik többé feltörhetetlennek a terméküket.

A pénztárca (wallet) programok azokat a biztonsági kódokat (tehát nem magát a virtuális pénzt, hanem a megfelelő privát kulcsokat) tárolják, amelyekkel a tulajdonos hozzáférhet saját címéhez, és akár tranzakciókat is indíthat a segítségével. Ezen belül többfajta, különféle eszközökre tervezett tárcatípusból választhatunk. A szoftver alapú tárcák egyik funkciója a „cold storage", ami a kulcsok offline védelmét biztosítja, hogy azokhoz senki se férhessen hozzá a hálózaton keresztül; léteznek ezen felül kifejezetten hardver alapú megoldások is, amelyek elektronikusan tárolják a kódokat.

A Bitfi nevű kriptowallet nemrég azzal került be a hírekbe, hogy feltörhetetlen védelemmel hirdette magát. A gyártó reklámarca ráadásul az a *John McAfee*, akinek a neve az utóbbi időben nem feltétlenül vált a minőség szinonimájává. Így nem kis visszhangot keltett, amikor McAfee először 100 ezer, később a társaság további 250 ezer dollárt ajánlott fel a júliusban piacra kerülő tárca első sikeres feltöréséért – pontosabban a gyártótól igényelhető, 50 bitcoinnal feltöltött eszközök kifosztásáért.

A rootolás egy vasat sem ért

A kísérletekre nem is kellett sokat várni. A 120 dolláros eszközt legelőször is darabokra kapták, hogy kiderüljön: a „világ legszofisztikáltabb műszere" tulajdonképpen egy némileg átalakított androidos telefon, amit a hardveres komponensek alapján összességében 35 dollár értékűre becsültek. A készülék ráadásul semmilyen védelemmel nincs ellátva a fizikai módosításokkal szemben: körömmel lepattintható a hátsó borítása, meg lehet piszkálni a hardverét, majd vissza lehet tenni a mit sem sejtő tulajdonos zsebébe.

Aztán nemsokára sor került a Bitfi rootolására is, nem beszélve a többi hiányosságról, mint például a kijelző és a chipkészlet közti, titkosítatlan I2C kapcsolat kihasználásáról, a fájlrendszer „dumpolásáról", a felhasználói adatokat gyűjtögető és továbbküldő szoftverről. Ezekért a Bitfi szerint azonban nem jár semmilyen jutalom: bár a „hibátlan, áthatolhatatlan biztonságot" emlegető gyártó valóban a bitcoinok átutalásáért tűzte ki a díjat, az egész kihívás nagyon gyorsan elkezdett komikussá válni.

A Bitfi és McAfee reakciói nemrég a legcikibb kereskedői magatartásért járó Pwnie-díjat is elhozták a Black Hat biztonsági konferencián, aztán augusztus végén kiderült: a bitcoinokat tényleg el lehet lopni a Bitfi tulajdonosaitól. Az eszköz egyébként – elvileg – nem tárolja a hozzáféréshez szükséges aktuális kulcsot, az azonosítás a titkos jelszó és a salt (egy véletlen bitsorozat) segítségével valósul meg. Mindez azonban nem sokat ér, ha a fizikai hozzáférést szerző támadó ki tudja nyerni a megfelelő kulcsokat, amelyeket a Bitfi a kelleténél jóval hosszabban tárol, még azután is, ha a felhasználó kikapcsolta a készüléket.

Erre már mehet a 250 ezer dollár

A sikeres „cold boot" hacket azóta hitelesítették is, így a Bitfi vezetőinek sem maradt sok választása, mint ötösből kettesbe váltani a korábbi hisztérikus hangnemről. Visszavonták a 250 ezres hibavadász jutalmat, amíg egy felbérelt külső szakértő megvizsgálja a sikeresnek mondott támadást (ennek részleteit egyébként a hackerek sem hozták nyilvánosságra, tekintettel a Bitfi néhány ezresre becsült felhasználói bázisára), és eltávolították olda-

lukról a "feltörhetetlen" védelmet ígérő szövegeket is. McAfee egy videointerjúban magyarázta, hogy az egész kampányra csak a hírverés miatt volt szükség, a Bitfi képviselője pedig majdhogynem könyörögve magyarázta, hogy a cégnek semmi sem fontosabb az ügyfelek biztonságánál.

A Bitfi dolga innentől nem lesz könnyű. A termékvisszahívás nemigen jön szóba, hiszen az eszközök a jelek szerint valóban tárolják a biztonsági kulcsokat, a szakértők szerint pedig egy firmware-frissítéssel sem lehet megoldani a problémát, mivel a Bitfi wallet olcsó Mediatek chipkészletet egyszerűen nem ilyen célú alkalmazásra tervezték, így bizonyos funkciói nem tilthatók vagy módosíthatók a firmware-en keresztül.

A tanulságot viszont könnyű lesz levonni: ha korábban még Oracle-szintű cégek is ráfaragtak a feltörhetetlen termékekkel való hencegésre, akkor egy startup számára sem biztos, hogy ez a legjobb módja a figyelem felkeltésének.

Ez a cikk független szerkesztőségi tartalom, mely a T-Systems Magyarország támogatásával készült. Részletek:
https://bitport.hu/impresszum#szponzoracioChromeHTML\Shell\Open\Command

Forrás: **https://bitport.hu/megint-feltortek-a-feltorhetetlen-penztarcat**

Válogatta: Fonyó Istvánné