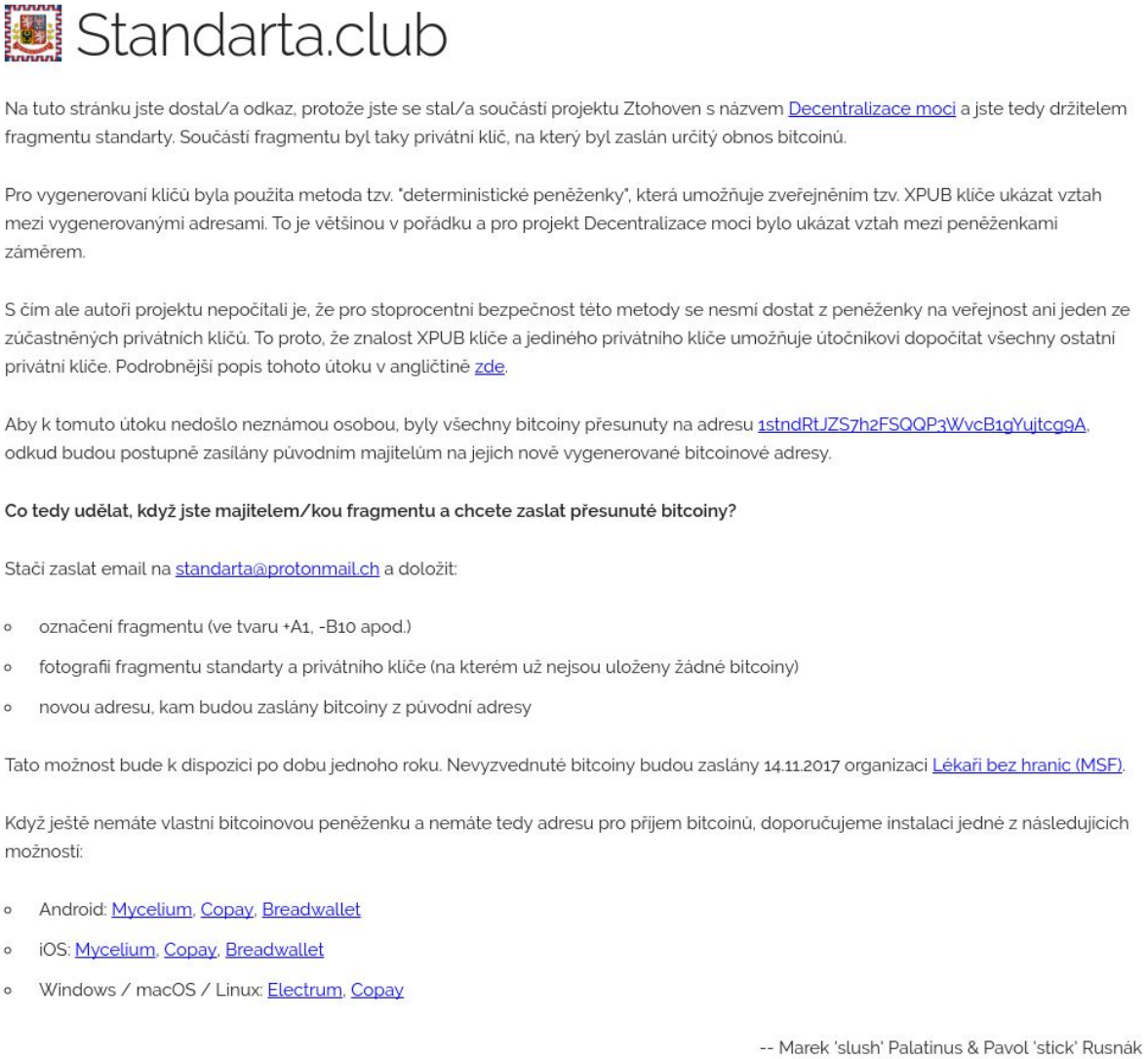
After we swept the coins and completed long negotiations with Ztohoven, we created a website hosted at standarta.club (standarta being the Czech word for the presidential flag) where we explained the technical vulnerability and most importantly the fact it was us who sweeped the coins stored on the fragments (the site mentioned our full names). The site also contained information that we created a new fund address from where we'll be sending coins to the original owners if they follow the claim procedure described on the website. Coins unclaimed for 1 year were supposed to be donated to the Czech chapter of Médecins Sans Frontières (MSF).

This agreed upon solution was not ultimately accepted by Ztohoven, because it was considered too complicated for people and they strongly preferred to handle the sensitive matter internally. We were asked to return the coins directly to Ztohoven, because they had already donated the same amount to MSF on their behalf. The fact that coins were indeed donated to MSF is also mentioned in the first paragraph of the Ztohoven project's website still available as of today (archived version).

We complied with the request of returning the coins to Ztohoven and shutting down the standarta.club website and considered the case closed.

Appendices

1) screenshot of the standarta.club website just before it was taken down in November 2016



Standarta.club

Na tuto stránku jste dostal/a odkaz, protože jste se stal/a součástí projektu Ztohoven s názvem Decentralizace moci a jste tedy držitelem fragmentu standarty. Součástí fragmentu byl taky privátní klíč, na který byl zaslán určitý obnos bitcoinů.

Pro vygenerovaní klíčů byla použita metoda tzv. "deterministické peněženky", která umožňuje zveřejněním tzv. XPUB klíče ukázat vztah mezi vygenerovanými adresami. To je většinou v pořádku a pro projekt Decentralizace moci bylo ukázat vztah mezi peněženkami záměrem.

S čím ale autoři projektu nepočítali je, že pro stoprocentní bezpečnost této metody se nesmí dostat z peněženky na veřejnost ani jeden ze zúčastněných privátních klíčů. To proto, že znalost XPUB klíče a jediného privátního klíče umožňuje útočníkovi dopočítat všechny ostatní privátní klíče. Podrobnější popis tohoto útoku v angličtině zde.

Aby k tomuto útoku nedošlo neznámou osobou, byly všechny bitcoiny přesunuty na adresu 1stndRtJZS7h2FSQQP3WvcB1gYujtcg9A, odkud budou postupně zasílány původním majitelům na jejich nově vygenerované bitcoinové adresy.

Co tedy udělat, když jste majitelem/kou fragmentu a chcete zaslat přesunuté bitcoiny?

Stačí zaslat email na standarta@protonmail.ch a doložit:

- označení fragmentu (ve tvaru +A1, -B10 apod.)
- fotografii fragmentu standarty a privátního klíče (na kterém už nejsou uloženy žádné bitcoiny)
- novou adresu, kam budou zaslány bitcoiny z původní adresy

Tato možnost bude k dispozici po dobu jednoho roku. Nevyzvednuté bitcoiny budou zaslány 14.11.2017 organizaci Lékaři bez hranic (MSF).

Když ještě nemáte vlastní bitcoinovou peněženku a nemáte tedy adresu pro příjem bitcoinů, doporučujeme instalaci jedné z následujících možností:

- Android: Mycelium, Copay, Breadwallet
- iOS: Mycelium, Copay, Breadwallet
- Windows / macOS / Linux: Electrum, Copay

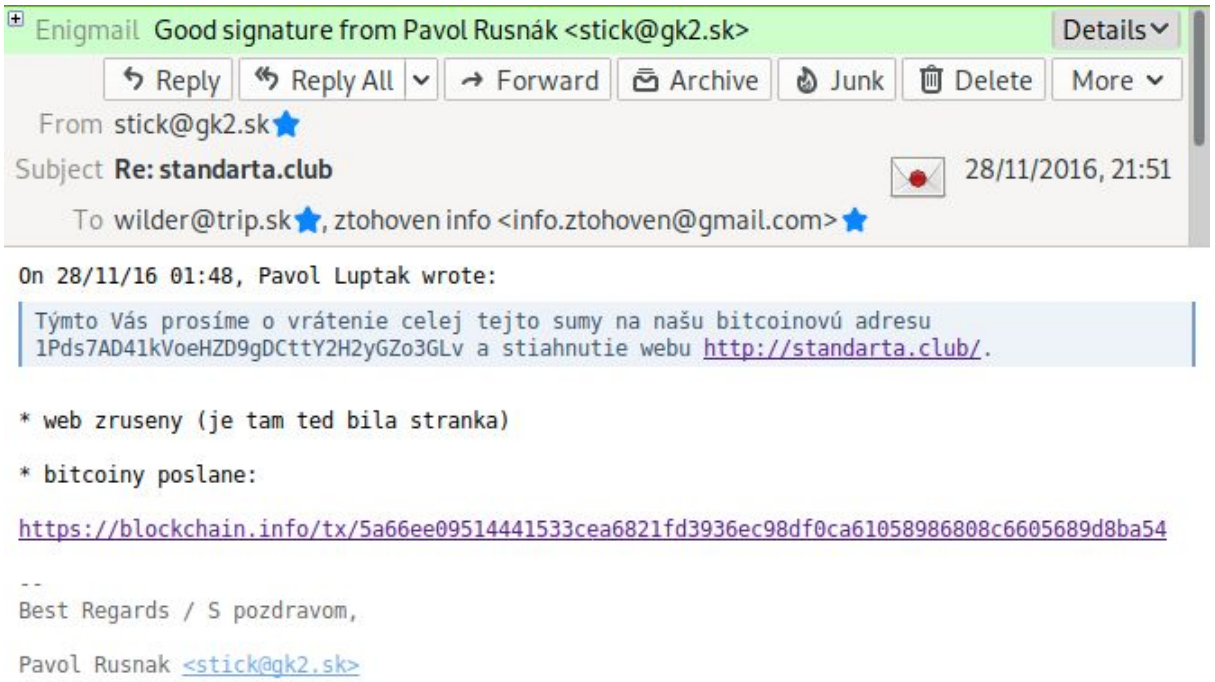
-- Marek 'slush' Palatinus & Pavol 'stick' Rusnák

image download: https://i.imgur.com/DDIzfgN.png

hash of the image:
cc88811c0a561694f3c44073b3af46bd9d7ffbcfd6ee214e382756fb31b04c02

proof of existence of the image on Bitcoin blockchain from November 2016:
https://btc1.trezor.io/tx/b9952d161139330baaa5234f50c22eaccb312ff7a6d8a541df2e4616549751fe

2) email where we comply with both requests asked by Ztohoven: to return the coins and to shutdown the standarta.club website



3) transaction where we sent all coins from the standarta.club fund address to the address requested by Ztohoven from email above

https://btc1.trezor.io/tx/5a66ee09514441533cea6821fd3936ec98df0ca61058986808c6605689d8ba54