How a loss of 3000BTC paved the way for the first hardware wallet 9 years ago

16th March 2021, Prague, Czech Republic — As Bitcoin hit a new all time high over the weekend - currently oscillating around 60 thousand dollars, the public and institutions are once again raising their interest. With this trend SatoshiLabs, the inventor of the first hardware wallet, are raising awareness about the need for protection and security among new cryptocurrency investors. Over the past decade, hundreds of thousands of Bitcoin have been lost or stolen because they were not properly secured, and the scale of these losses in dollar terms is reaching unbelievable amounts.

For every success story, there are many more tales of loss...

In March it was just over 9 years ago the british cloud hosting service Linode, which was running the world's first bitcoin mining pool, SlushPool, was hit by an attacker. A hot (online) wallet holding 3000 BTC for payouts to miners, was emptied, leaving the pool operator, Marek Palatinus (Slush) the CEO of SatoshiLabs and inventor of Trezor, to compensate the losses from his own funds. In total, 50,000 bitcoin were lost by Linode users, making it one of the biggest bitcoin thefts at the time. The losses in fiat terms were significant, totalling around $20,000 for SlushPool alone. Had they been secured properly, they'd now be worth around $180,000,000.

"This incident and many other stories out there should remind everyone that keeping Bitcoin on any online service like exchange is an unnecessary risk. You are always exposed to the potential of total loss, but in self custody, you can better evaluate the risk and you don't depend on third party negligence. Coins that are not part of an active trade should be kept in cold storage using a hardware wallet, where they can be conveniently accessed without being exposed to a network."

— Marek Palatinus (Slush), CEO of SatoshiLabs

How is cryptocurrency stored?

The Trezor hardware wallet was created to give Bitcoiners an easy, comprehensive way to protect cryptocurrency investments, without needing to understand how everything works.

The function of a hardware wallet is simple: it creates the secret keys that unlock cryptocurrency, and it does so entirely offline. Since the keys are kept isolated in the physical world and the coins are digital, it becomes practically impossible for someone else to get hold of them. If the keys are created on a Trezor, the coins are safe against all known external threats. Most major crypto crimes happen on hot wallets or exchanges!

Using Bitcoin keeps getting easier

Bitcoin is **decentralized**, which means it depends on contributions from lots of different people working independently or in small groups all over the world. While this keeps it

Kristýna Mazánková, Head of PR
kristyna.mazankova@satoshilabs.com

secure and not controlled by anyone, it means the ecosystem of tools used with Bitcoin have developed independently as well, at different rates of progress.

- **Exchanges holding your coins**

It's clear that keeping coins on an exchange is a bad idea, even the most popular exchange in the world. But it comes down to where the user keeps the keys: if they're on a network, they can be stolen.

Blog - Why you should not store cryptocurrency on exchanges

- **Protect the seed**

The offline backup that lets you recover the wallet, known as a seed, must be kept in the physical world. If it ends up on a network, all the funds can be taken. Using a Trezor, the theft-resistant seeds that never touch the internet can be made.
Although the seed is kept offline, phishing is a threat. Using cloned websites or fake apps, phishing attacks trick many into giving away the seed voluntarily. Trezor devices will always tell you if and how to use the seed, so everything else can be ignored and reported. In recent months, phishing emails and texts have been on the rise as have fake apps. There is currently no official Trezor mobile app on any app marketplace so please report any fake application you find.

Blog - Staying safe from crypto scams and phishing

- **Use secure authentication**

SMS authentication is widespread but very insecure due to how easy it is to swap someone's SIM to steal their phone number. Google authenticator and other time-based code generators are also not secure. Modern security standards such as FIDO U2F and FIDO2 are much safer because they don't rely on a shared key. Trezor can be used as FIDO authenticator and make sure that email and other sensitive accounts are properly secured.

Video - https://www.youtube.com/watch?v=a7UO_OjMmLQ

About SatoshiLabs:

SatoshiLabs is a privately held company founded in 2013 and based in the Czech Republic. The first company product was the world's first cryptocurrency hardware wallet. Its popular flagship product, the Trezor Model T, introduced new measures of security such as its full-color touchscreen. SatoshiLabs is also the creator of more than 22 innovative security standards like Recovery seed, Passphrase, or Shamir Backup, which are significantly improving the whole industry of online security. Present in over 220 countries worldwide, SatoshiLabs remains open-source, making the best security solutions accessible to anyone, anywhere. More information at www.satoshilabs.com and www.trezor.io

Kristýna Mazánková, Head of PR
kristyna.mazankova@satoshilabs.com