Bitcoin Wallets

Alex Khodaverdian
Class Survey

- How many of you have heard of Bitcoin/Ethereum/Cryptocurrencies?
  - (Probably everyone)
- How many of you own:
Class Survey

- How many of you have heard of Bitcoin/Ethereum/Cryptocurrencies?
  - (Probably everyone)

- How many of you own:
  - Bitcoin
Class Survey

- How many of you have heard of Bitcoin/Ethereum/Cryptocurrencies?
  - (Probably everyone)
- How many of you own:
  - Bitcoin
  - Ethereum
Class Survey

● How many of you have heard of Bitcoin/Ethereum/Cryptocurrencies?
  ○ (Probably everyone)

● How many of you own:
  ○ Bitcoin
  ○ Ethereum
  ○ Other Altcoins?
Class Survey

● How many of you have heard of Bitcoin/Ethereum/Cryptocurrencies?
  ○ (Probably everyone)

● How many of you own:
  ○ Bitcoin
  ○ Ethereum
  ○ Other Altcoins?

● Where do you store your cryptocurrencies?
Class Survey

- How many of you have heard of Bitcoin/Ethereum/Cryptocurrencies?
  - (Probably everyone)

- How many of you own:
  - Bitcoin
  - Ethereum
  - Other Altcoins?

- Where do you store your cryptocurrencies?
  - Coinbase/Binance/Any other centralized exchange
Class Survey

- How many of you have heard of Bitcoin/Ethereum/Cryptocurrencies?
  - (Probably everyone)
- How many of you own:
  - Bitcoin
  - Ethereum
  - Other Altcoins?
- Where do you store your cryptocurrencies?
  - Coinbase/Binance/Any other centralized exchange
  - Hardware Wallet? (Trezor, Ledger)
Class Survey

- How many of you have heard of Bitcoin/Ethereum/Cryptocurrencies?
  - (Probably everyone)
- How many of you own:
  - Bitcoin
  - Ethereum
  - Other Altcoins?
- Where do you store your cryptocurrencies?
  - Coinbase/Binance/Any other centralized exchange
  - Hardware Wallet? (Trezor, Ledger)
  - Desktop Wallet? (Electrum, Multibit)
What is a Bitcoin Wallet?

- Broadly speaking, a Bitcoin Wallet performs these three tasks:
  - A public key distribution program (i.e. Generating addresses)
  - A signing program (i.e. Signing a Transaction)
  - A network program (i.e. Receiving information from the blockchain and broadcasting new transactions)

- Types of Wallets?
  - Full-Service Wallets
  - Signing Only Wallets
    - Offline Wallets
    - Hardware Wallets
  - Distributing-Only Wallets

- Main Security Concern?
  - Compromising Private Keys
Full Service Wallets

● What do they do?
  ○ Generate Private Keys
  ○ Derive Corresponding Public Keys
  ○ Help distribute public keys
  ○ Monitor for outputs sent to those public keys
  ○ Create and Sign transactions
  ○ Broadcast the signed transactions

● What is the problem with a full service wallet?
  ○ Private keys stored on device connected to the internet

● Partial Solution?
  ○ Encrypt wallet files
  ○ Can’t protect against attacks designed to capture key from memory
I woke up and found my Exodus wallet hacked and cleared.

So long story short... A few days ago, I woke up, made an extra large cup of black Colombian coffee. I was checking CoinMarketCap, rubbing my hands and enjoying magnificent green charts. However, this euphoric feeling ended shortly when I decided to check my Exodus wallet, which I use to keep a part of my portfolio. And surprise, surprise it was fucking empty! My cryptos transferred to this motherfucker’s account - https://etherscan.io/txs?a=a0xb643b3e10731a1d84391a8d1b33775629464b43p=1

I have a couple of hypotheses, how the motherfucker managed to hack the wallet. Through my own stupidity, somehow I forgot to delete a screenshot of backup words on my personal Google Drive. I know - a dumb, ignorant move on my part. Or my machine (it has OSK and Avast installed) was compromised, maybe some kind of keylogger installed.

That being said, I’ve learned my lesson. Ledger Nano S is on my way. I don’t want any more surprises in the morning.

Now the question is, what can be done with the motherfucker, who stole the funds? As you can see, more than $200K was hacked from multiple persons and laundered via https://hitbtc.com. Should I reach out to Hitbtc? Report it to legal authorities?
Full Service Wallets

I woke up and found my Exodus wallet hacked and cleared.

August 24, 2017, 12:33:09 PM

So long story short... A few days ago, I woke up, made an extra large cup of black Colombian coffee. I was checking CoinMarketCap, rubbing my hands and enjoying magnificent green charts. However, this euphoric feeling ended shortly when I decided to check my Exodus wallet, which I use to keep a part of my portfolio. And surprise, surprise it was fucking empty! My cryptos transferred to this motherfucker’s account - https://etherscan.io/address=0xf68649e0e073a11d68391dd1b37b639464d438p=1

I have a couple of hypotheses, how the motherfucker managed to hack the wallet. Through my own stupidity, somehow I forgot to delete a screenshot of backup words on my personal Google Drive. I know - a dumb, ignorant move on my part. OR my machine (it has DXS and Avast installed) was compromised, maybe some kind of keylogger installed.

That being said, I’ve learned my lesson. Ledger Nano S is on my way. I don’t want any more surprises in the morning.

Now the question is, what can be done with the motherfucker, who stole the funds? As you can see, more than $200K was hacked from multiple persons and laundered via https://bitclic.com. Should I reach out to Hitbtc? Report it to legal authorities?
Full Service Wallets
Signing Only Wallets

- How do we better protect our private keys?
  - Generate and store private keys in a separate wallet
  - Work with a networked wallet to interact with Bitcoin network

- Types of Signing Only Wallets?
  - Offline Wallet
    - I.e. stored on an offline computer
    - Distribute public keys to receive payment
    - Save unsigned transactions to removable media, load on offline instance, sign it, and save it back to removable media
    - Open signed transaction in online instance and broadcast
  - Hardware Wallet
    - Private Keys stored on hardware device (i.e. Trezor)
    - Prompt for confirmation on hardware device before signing transaction
Hierarchical Deterministic Key Creation

- Is Bitcoin anonymous?
  - No. Why?
    - If an address is linked to illegal activity, and later, through a series of transactions, ends up on a website which knows your identity, you can be exposed to authorities.
    - Sheep Marketplace
Hierarchical Deterministic Key Creation

- Is Bitcoin anonymous?
  - No. Why?
    - If an address is linked to illegal activity, and later, through a series of transactions, ends up on a website which knows your identity, you can be exposed to authorities.
    - *Sheep Marketplace*
      
      It then details how two Department of Homeland Security special agents named only as Johnston and Gino used the website *Blockchain.info*, which publicly displays bitcoin transactions, to track the movement of the stolen bitcoins across various addresses, including one assigned by Coinbase.

      In response to a subpoena, Coinbase revealed the owner of that address was Gibson, that the account was linked to one at Bancorp Bank and that from late December 2013 to late January 2014, Gibson had deposited more than 842 bitcoins valued at more $646,000.
Hierarchical Deterministic Key Creation

● Is Bitcoin anonymous?
  ○ No. Why?
    ■ If an address is linked to illegal activity, and later, through a series of transactions, ends up on a website which knows your identity, you can be exposed to authorities.
    ■ **Sheep Marketplace**

● What if we could generate multiple addresses, without anyone knowing they are linked, with just one private key?

● Process?
  ○ Generate parent private key
  ○ Derive parent public key
  ○ $\text{point}( (\text{parent\_private\_key} + 1) \mod p ) = \text{parent\_public\_key} + \text{point}(1) = \text{child\_public\_key}_1$
  ○ $\text{point}( (\text{parent\_private\_key} + 2) \mod p ) = \text{parent\_public\_key} + \text{point}(2) = \text{child\_public\_key}_2$
Hierarchical Deterministic Key Creation
Hierarchical Deterministic Key Creation
Hierarchical Deterministic Key Creation

- **Problems with this?**
  - If you know one child public key, you can discover all other keys created by the parent public key.

- **Solution:**
  - In addition to parent private key and public key (256 bits), generate a chain code that’s 256 bits, along with a given index.
  - Extended keys: Private key + Chain Code, Public Key + Chain Code.
  - Feed parent private key, chain code, and index into HMAC-SHA512 function to generate offset and child chain code.

- So we can’t easily link addresses generated from a parent public key easily, but are we now anonymous?
  - No (Ex: 5 separate addresses known for accepting payments for illicit goods are found to converge to a single address after several payments).
Creation Of The Master Keys
Normal Hierarchical Deterministic (HD) Key Derivation (BIP32)
Discussion

- If you adequately secure your private keys digitally, are your funds still safe?
Discussion

- If you adequately secure your private keys digitally, are your funds still safe?
  - Physical Extortion
Discussion

- If you adequately secure your private keys digitally, are your funds still safe?
  - Physical Extortion

Russia: Blogger Who ‘Boasted’ About Crypto Wealth Beaten and Robbed For $425k
Discussion

- If you adequately secure your private keys digitally, are your funds still safe?
  - Physical Extortion

Russia: Blogger Who ‘Boasted’ About Crypto Wealth Beaten and Robbed For $425k

Bitcoin exchange chief kidnapped as he leaves work
Discussion

- If you adequately secure your private keys digitally, are your funds still safe?
  - Physical Extortion
  - Scams meant to separate you from your crypto
Discussion

- If you adequately secure your private keys digitally, are your funds still safe?
  - Physical Extortion
  - Scams meant to separate you from your crypto

Texan gets one-and-a-half years in prison for running bitcoin Ponzi scheme

NEW YORK (Reuters) - A Texas man was sentenced to one-and-a-half years in prison on Thursday for operating a bitcoin-related Ponzi scheme that prosecutors say resulted in the first U.S. criminal securities fraud case related to the digital currency.
Discussion

- If you adequately secure your private keys digitally, are your funds still safe?
  - Physical Extortion
  - Scams meant to separate you from your crypto
- If you’re involved in illegal activities, would you use Bitcoin?
Discussion

- If you adequately secure your private keys digitally, are your funds still safe?
  - Physical Extortion
  - Scams meant to separate you from your crypto
- If you’re involved in illegal activities, would you use Bitcoin?
- If a reputable exchange holds your Bitcoin, are your funds safe?