Measuring Bitcoin-based Cybercrime

Marie Vasek
Dissertation Defense
29 March 2016
Thesis Contributions and Talk Outline

• Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.
  
  • Ch. 2 - Bitcoin Primer (covered in proposal)
  • Research Questions (covered in proposal)
  • Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
  • Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
  • Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
  • Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
  • Ch. 7 - Conclusions
Thesis Contributions and Talk Outline

- Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.

- **Ch. 2 - Bitcoin Primer (covered in proposal)**
- **Research Questions (covered in proposal)**
- **Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)**
- **Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)**
- **Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)**
- **Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)**
- **Ch. 7 - Conclusions**
Bitcoin

- Bitcoin is a **public, digital, decentralized** currency.

- Public
  - Every transaction (past or current) can be read by anybody.

- Digital
  - There are no bills, only bits to represent transactions.

- Decentralized
  - Bitcoins are mined, not minted, by a collection of actors, not a central bank.
  - Anybody can create an account and receive bitcoin.
  - Anybody can try to mine bitcoin.
  - Rules are set by computer code and changed upon a consensus of the actors.
This server supports keyword search. We welcome your electronic feedback about our server!

We support the Golden Key campaign of the Internet Privacy Coalition.

Parts copyright © 1990-1996 by DigiCash bv; DigiCash and ecash are trademarks.
Featured Merchants

Marketiva.com — Popular Forex company!
Instaforex.com — Award winning forex.
Masterforex.org — Award winning forex.

Featured Exchange Services

wm-center.com (English, Russian) — Fast and reliable service 24/7.
e-Naira.com (English) — Reputable exchanger located in Africa.
ExchangeZone.com (English)

Wholesale Exchange Services

eCardOne.com (English, Italian, Spanish, German, Czech) — Authorized reseller, official debit card provider
SwiftExchanger.com (English) — Official Liberty Reserve merchant wholesaler

Quick Payments

An easy access to your funds to make payments quickly.

This feature allows you to make quick payments without accessing your main Liberty Reserve account. Just set daily, weekly or monthly limit of funds you wish to use for handy Quick Payments and do transfers to your partners quickly and safely.

Live Chat

Have questions? Liberty Reserve provides personal, live, one-to-one chat with a customer support representative to answer your questions. No more waiting hours or days to get a simple question answered. Our representatives can also push a URL onto your computer as a pop-up so that you do not have to go looking for a particular link.

You can also get the chat history automatically emailed to you!
Online Currency Exchange Accused of Laundering $6 Billion

By MARC SANTORA, WILLIAM K. RASHBAUM and NICOLE PERLROTH  MAY 28, 2013

The operators of a global currency exchange ran a $6 billion money-laundering operation online, a central hub for criminals trafficking in everything from stolen identities to child pornography, federal prosecutors in New York said on Tuesday.
Why Scammers Use Bitcoin

• Lower fees (more profit for criminals)
• Large userbase (compared to other digital currencies)
• Easy to get (can exchange Bitcoin for cash on the street)
• Distributed system (no Bank of Bitcoin to forcibly shut down)
• Less direct regulatory oversight (anti-money laundering efforts only on some endpoints)

I use the public nature of Bitcoin to directly measure cybercrime.
Thesis Contributions and Talk Outline

• Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.

  • Ch. 2 - Bitcoin Primer (covered in proposal)
  • **Research Questions** (covered in proposal)
  • Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
  • Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
  • Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
  • Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
  • Ch. 7 - Conclusions
Security Economics

- Security economics literature has identified several key reasons for security failure:
  - incentives: profit motivated attackers [Ch. 3-6]
  - information asymmetries: hard to ascertain whether service is legitimate or not [Ch. 4-5]
  - externalities: when harm is directed elsewhere; DDoS attacks [Ch. 3]; can’t trust the ecosystem [Ch. 4]
Cybercrime Measurement

• Large body of research on improving understanding of how cybercriminals operate so that we might more effectively dismantle their networks:
  • DDoS attacks: existing work measuring, categorizing DDoS attacks
  • HYIPs: Moore et al. monitored over 1000 scams and estimated their profits using inferred approximations
  • Passwords: existing work on password dumps, which passwords are being used, frequency of password use
• This thesis contributes to the knowledge on these threats by studying their prevalence in the Bitcoin ecosystem
Publications

• In dissertation:

• Other publications:
  • Marie Vasek and Tyler Moore. "Empirical Analysis of Factors Affecting Malware URL Detection". In 8th APWG eCrime Researchers Summit (eCrime), September 2013.
  • Marie Vasek and Tyler Moore. "Do Malware Reports Expedite Cleanup? An Experimental Study". In 5th USENIX Workshop on Cyber Security Experimentation and Test (CSET), Berkeley, CA, August 2012.
Thesis Contributions and Talk Outline

• Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.

  • Ch. 2 - Bitcoin Primer (covered in proposal)
  • Research Questions (covered in proposal)
  • **Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)**
  • Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
  • Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
  • Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
  • Ch. 7 - Conclusions
Research Contributions

• Method to collect cybercrime data:
  • Inferring DDoS attacks from user reports
  • Reliable estimation of attack targets and date

• Analysis of gathered data:
  • Summary statistics of prevalence over time
  • Quantifying impact of attacks (on mining pools and exchanges)
Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem

Topic: BTC GUILD Down because of DDOS Attack (Read 1611 times)

BTC GUILD Down because of DDOS Attack
July 05, 2011, 02:02:53 PM

BTC Guild down because of ddos attack?
can someone from BTC Guild let us know whats going on, please?

Author: Kris
Donator
Hero Member
_activity: 645

Topic: 2012-09-15 walletbit.com - WalletBit Under DDOS - 1000BTC Demanded (Read 518 times)

2012-09-15 walletbit.com - WalletBit Under DDOS - 1000BTC Demanded
September 21, 2012, 05:13:46 PM

Quote
The WalletBit website and service came under DDOS attack on September 15, 2012, completely disabling the services as of around 9:00 PM GMT.

Source: http://bitcoinmagazine.net/walletbit-under-ddos-1000btc-demanded/
Reported DDoS over time by category
Chapter 3 Conclusions

• Developed methodology for measuring DDoS on Bitcoin services
• Found circumstantial evidence for profit-motivated DDoS attacks on the Bitcoin ecosystem
• Data produced for this chapter already used by other researchers to advance understanding of DDoS impact
  • Feder et al. (WEIS 2016) found that the distribution of the daily trading volume at Mt. Gox becomes less skewed (fewer big trades) after DDoS attacks
Thesis Contributions and Talk Outline

• Thesis: We measure cybercrime activity in the Bitcoin ecosystem to better understand attacker motivation and efficacy of various crimes and countermeasures.

  • Ch. 2 - Bitcoin Primer (covered in proposal)
  • Research Questions (covered in proposal)
  • Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
  • **Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)**
  • Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
  • Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
  • Ch. 7 - Conclusions
Research Contributions

• Method to collect cybercrime data:
  • Find candidate scams using aggregated defender data
  • Confirm scams through manual inspection
  • Measure money in/out of scams using data from the public Bitcoin blockchain

• Analysis of gathered data:
  • Construct taxonomy of scam categories and document prevalence and revenues
  • Provide first longitudinal analysis of HYIP cash flows and victim losses
Measuring the Profits of Bitcoin Scams

[SCAM] Leancy Ltd - Bitcoin Investment - 150% Return & 5% Daily Interest

LEANCY HAS NOT BEEN PAYING SINCE 03/11/14. NO ADMINS COULD BE REACHED. DO NOT DEPOSIT ANY FUNDS INTO LEANCY.

FortuneJack.com
No.1 Online Cryptocurrency Casino

1 BTC Welcome Bonus Up to 1 Day Binary Trading Live Roulette Live Sic Bo Provably Fair Games Start WINNING Now

PORTALS
Facebook Group (Leancy Investors) - A place (free of spam) for honest discussions regarding Leancy and other HYIPs and it's Illegal operations as well as news and updates regarding any information on those behind the scams.

Skype Room - Unfortunately, bitcointalk isn't displaying the link properly so if you want to join, you'll have to add the Skype users: leancytlc and include in the request message you're from bitcointalk. This chat room has the same intent as the FB group above.
Profits of Ponzis

Daily payments into and out of Bridge HYIPs

- Payments in (all Bridge HYIPs)
- Payments out (all Bridge HYIPs)

Daily payments in and out (BTC)

Payments in
- Rockwell Partners
- Minimalism10
- Twelverized
- Leancy
- Ro Invest
- Fin Mutual
- Bitcoin Arbs
- Craigslist Investment
- cryptory
Bitcoin Wallet Scams

Welcome to EasyCoin.net Bitcoin Wallet

Now with free Bitcoin mixer, you will always get new coins back when you withdraw from your EasyCoin.net wallet!
You only pay the Bitcoin transaction fee (0.001 BTC).
We also support completely free account to account transfers.

→ Click here to sign up now!
Bitcoin Wallet Scams: Profit

Weekly Payout to Scam Wallets

Transaction Volume (BTC)

Transaction Volume (USD)
Chapter 4 Conclusions

- Developed manually intensive methodology for measuring profits of Bitcoin scams
- Found $11 million revenue over 42 scams
- Indirect harm from scams — undermine trust in the Bitcoin ecosystem
Thesis Contributions and Talk Outline

• Thesis: We measure cybercrime activity in the Bitcoin ecosystem to better understand attacker motivation and efficacy of various crimes and countermeasures.

• Ch. 2 - Bitcoin Primer (covered in proposal)
• Research Questions (covered in proposal)
• Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
• Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
  • **Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams** (new)
  • Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
• Ch. 7 - Conclusions
Research Contributions

• Method to collect cybercrime data:
  • Gather candidate scam data directly from scammer advertising venues
  • Automatically confirm scams by inspecting payout mechanisms
  • For confirmed scams, collect usage, performance and demographic indicators from forum posts

• Analysis of gathered data:
  • Describe supply-side characteristics of scams, scammers
  • Describe demand-side characteristics of victims
# Ch 4 and Ch 5 Differences

<table>
<thead>
<tr>
<th>Ch 4</th>
<th>Ch 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify candidate scams using aggregate defender data</td>
<td>Identify candidate scams using attacker advertisement sources</td>
</tr>
<tr>
<td>False positives are not scams</td>
<td>False positives are postings which are about gambling</td>
</tr>
<tr>
<td>Only include scams with Bitcoin addresses</td>
<td>Only include scams with URLs or Bitcoin addresses</td>
</tr>
<tr>
<td>Manually intensive scam identification</td>
<td>Semi-automated scam identification</td>
</tr>
<tr>
<td>Consider a variety of scam types</td>
<td>Only consider Ponzi schemes</td>
</tr>
</tbody>
</table>
Measuring the Supply and Demand for Bitcoin Scams

---

**MANOJBASHU**

Newbie

**GET 100X BITCOIN INVESTMENT IN 24 HOURS**

March 30, 2015, 04:15:31 PM

GET 100X BITCOIN INVESTMENT IN 24 HOURS

http://bitcoin-profit.site.bz

---

**TECH-TOOLS**

Newbie

**Re: GET 100X BITCOIN INVESTMENT IN 24 HOURS**

November 19, 2015, 05:25:43 AM

I did sent 0.2 and I got nothing back!!!

Status: 171 confirmations
Date: 11/17/15 20:52
To: 100x 19BtpFr6kWqYyqoAmSv5d2TZ4uwH56dCd
Debit: -0.20000000 BTC
Transaction fee: -0.00004070 BTC
Net amount: -0.20004070 BTC
Data Collection Methodology

- Crawled 11,424 threads on the three subforums of bitcointalk.org:
  - Scam accusations
  - Gambling: Games and Rounds
  - Gambling: Investment Games
- Refined this further to find 1,780 scams advertised through 1,804 ponzi-registered domains as well as 1,448 Bitcoin addresses collated from 2,617 threads.
Lifetime of Scams

![Survival Probability vs Days on Forum Graph](image)
Lifetime of Scams

![Graph showing survival probability over days on forum]
Scammer Interaction

Survival Probability

Days on Forum

- Only initial posting
- >0.25 of the comments
- >0.5 of the comments

Lifetime of Scams

Stages:
- Days on Forum
- Survival Probability
Identifying shills

• Shills: users which we believe are the attacker under a different name

• Finding ground truth on shills: manually inspect threads, look for unusually positive posters & strong but false or unverifiable information

• Use forum history (only posts about one scam) to identify most of these users
Shill Interaction

![Survival Probability Graph]

- Only initial posting
- Shill >0.10 of the comments
- Scammer >0.10 of the comments
- Scam or shill >0.25 of the comments

Days on Forum vs. Survival Probability

- Survival probability decreases as days on forum increase.
- The survival probability for different interaction types varies.
Scammer Forum History

Survival Probability

Days on Forum

Days on Forum

Old account
Same day account

Only One Scam
Only on Scam Posts
General Posting

Only One Scam
Only on Scam Posts
General Posting
Ponzi Victims over Time

Within a day | 1 day | 2–7 days | 8–14 days | 15–21 days | 22–28 days | 29–56 days | 57–112 days | >113 days
# Forum History of Ponzi Victims

<table>
<thead>
<tr>
<th>Category</th>
<th># Victim Posts</th>
<th># Other Posts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Altcoins (all)</td>
<td>32 536</td>
<td>5 429 022</td>
</tr>
<tr>
<td>Alternative Clients</td>
<td>106</td>
<td>54 159</td>
</tr>
<tr>
<td>Bitcoin Discussion</td>
<td>8 872</td>
<td>998 246</td>
</tr>
<tr>
<td>Development &amp; Technical Discussion</td>
<td>683</td>
<td>162 405</td>
</tr>
<tr>
<td>Group Buys</td>
<td>498</td>
<td>84 734</td>
</tr>
<tr>
<td>Hardware</td>
<td>2 730</td>
<td>518 728</td>
</tr>
<tr>
<td>Mining</td>
<td>427</td>
<td>1 044 148</td>
</tr>
<tr>
<td>Mining software (miners)</td>
<td>274</td>
<td>67 561</td>
</tr>
<tr>
<td>Mining speculation</td>
<td>616</td>
<td>63 071</td>
</tr>
<tr>
<td>Pools</td>
<td>885</td>
<td>177 985</td>
</tr>
<tr>
<td>Press</td>
<td>696</td>
<td>74 437</td>
</tr>
<tr>
<td>Project Development</td>
<td>1 526</td>
<td>137 245</td>
</tr>
<tr>
<td>Technical Support</td>
<td>586</td>
<td>58 952</td>
</tr>
<tr>
<td>Auctions</td>
<td>1 865</td>
<td>108 048</td>
</tr>
<tr>
<td>Collectibles</td>
<td>1 063</td>
<td>60 745</td>
</tr>
<tr>
<td>Computer hardware</td>
<td>1 462</td>
<td>118 584</td>
</tr>
<tr>
<td>Currency exchange</td>
<td>3 124</td>
<td>138 264</td>
</tr>
<tr>
<td>Digital goods</td>
<td>7 303</td>
<td>277 903</td>
</tr>
<tr>
<td>Economics</td>
<td>3 692</td>
<td>1 204 450</td>
</tr>
</tbody>
</table>
Forum History of Ponzi Victims

<table>
<thead>
<tr>
<th>Category</th>
<th>First Year</th>
<th>Second Year</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gambling</td>
<td>12070</td>
<td>1297038</td>
<td>(+)</td>
</tr>
<tr>
<td>Gambling discussion</td>
<td>5677</td>
<td>340593</td>
<td>(+)</td>
</tr>
<tr>
<td>Games and rounds</td>
<td>23331</td>
<td>388689</td>
<td>(+)</td>
</tr>
<tr>
<td>Goods</td>
<td>1251</td>
<td>587681</td>
<td>(-)</td>
</tr>
<tr>
<td>Investor-based games</td>
<td>15402</td>
<td>115454</td>
<td>(+)</td>
</tr>
<tr>
<td>Lending</td>
<td>3230</td>
<td>138108</td>
<td>(+)</td>
</tr>
<tr>
<td>Marketplace</td>
<td>517</td>
<td>5372844</td>
<td>(-)</td>
</tr>
<tr>
<td><strong>Micro Earnings</strong></td>
<td>3694</td>
<td>144797</td>
<td>(+)</td>
</tr>
<tr>
<td>Scam Accusations</td>
<td>4643</td>
<td>116151</td>
<td>(+)</td>
</tr>
<tr>
<td>Securities</td>
<td>1338</td>
<td>202813</td>
<td></td>
</tr>
<tr>
<td>Service Announcements</td>
<td>2338</td>
<td>288993</td>
<td>(+)</td>
</tr>
<tr>
<td>Service Discussion</td>
<td>3692</td>
<td>330535</td>
<td>(+)</td>
</tr>
<tr>
<td>Services</td>
<td>8528</td>
<td>407342</td>
<td>(+)</td>
</tr>
<tr>
<td><strong>Speculation</strong></td>
<td>5058</td>
<td>883584</td>
<td>(-)</td>
</tr>
<tr>
<td>Trading Discussion</td>
<td>1678</td>
<td>257930</td>
<td></td>
</tr>
<tr>
<td>Local (all)</td>
<td>14932</td>
<td>4454405</td>
<td>(-)</td>
</tr>
<tr>
<td>Archival</td>
<td>1026</td>
<td>147836</td>
<td></td>
</tr>
<tr>
<td>Beginners &amp; Help</td>
<td>3923</td>
<td>564720</td>
<td></td>
</tr>
<tr>
<td>Meta</td>
<td>1960</td>
<td>134319</td>
<td>(+)</td>
</tr>
<tr>
<td>Off-topic</td>
<td>8309</td>
<td>563710</td>
<td>(+)</td>
</tr>
<tr>
<td>Politics &amp; Society</td>
<td>2181</td>
<td>290782</td>
<td></td>
</tr>
</tbody>
</table>
Cox Proportional Hazards Model

• Lots of measurable variables seem to affect lifetime — but which variables are responsible?

• A proportional hazards model lets us disentangle the effects of various measures on lifetime.

• Dependent variable: lifetime

• Independent variables: explanatory factors
Cox Proportional Hazards Model: Independent Variables

- **daily # victim comments**
  - Number of victim comments over the lifetime of the scam.

- **daily # scammer comments**
  - Number of scammer comments over the lifetime of the scam.

- **shill has posted?**
  - True if a “shill” has posted anywhere in the thread. (30% of the time)

- **same day account**
  - True if the scammers’ bitcointalk account was registered the same day as the original post for the scam. (43% of the time)
Cox Proportional Hazards Model: Results

<table>
<thead>
<tr>
<th></th>
<th>coef</th>
<th>exp(coef)</th>
<th>95% CI</th>
<th>p value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily # victim comments</td>
<td>0.028</td>
<td>1.029</td>
<td>(1.022, 1.036)</td>
<td>&lt;&lt;0.0001</td>
</tr>
<tr>
<td>Daily # scammer comments</td>
<td>0.022</td>
<td>1.022</td>
<td>(1.002, 1.043)</td>
<td>0.034</td>
</tr>
<tr>
<td>Shill has posted?</td>
<td>-0.846</td>
<td>0.429</td>
<td>(0.385, 0.479)</td>
<td>&lt;&lt;0.0001</td>
</tr>
<tr>
<td>Same day account</td>
<td>0.374</td>
<td>1.1453</td>
<td>(1.320, 1.599)</td>
<td>&lt;&lt;0.0001</td>
</tr>
</tbody>
</table>

Log-rank test: $Q=4389.2$, $p<<0.0001$, $R^2 = 0.218$
Chapter 5 Conclusions

• Developed semi-automated methodology for finding Bitcoin Ponzi schemes

• Found over 1,700 of these scams, half of which end within a week of being started.

• Frequency of victim and scammer posts is negatively correlated with scam survival

• Forum history positively correlated with scam survival
Thesis Contributions and Talk Outline

• Thesis: We measure cybercrime activity in the Bitcoin ecosystem to better understand attacker motivation and efficacy of various crimes and countermeasures.

  • Ch. 2 - Bitcoin Primer (covered in proposal)
  • Research Questions (covered in proposal)
  • Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
  • Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
  • Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
  • Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
  • Ch. 7 - Conclusions
Research Contributions

• Method to collect cybercrime data:
  • Generate large corpus of candidate passwords/phrases
  • Efficiently use blockchain to study attacker draining behaviors

• Analysis of gathered data:
  • Use Bitcoin to quantify passphrase selection
  • Measure attacker draining performance using timing data
Measuring the Use and Abuse of Brain Wallets
Measuring the Use and Abuse of Brain Wallets
Bitcoin Wallets: a Universal Bug Bounty

“deadsheep”
Bitcoin Wallets: a Universal Bug Bounty

“deadsheep”
Measuring the Use and Abuse of Brain Wallets
Password Corpora:
3.9 trillion Candidate Passwords

<table>
<thead>
<tr>
<th>Source</th>
<th># Wallets</th>
<th>(non-empty)</th>
<th>Unique</th>
<th>90% # drains</th>
<th>Total BTC</th>
<th>Total USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word lists</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>xkcd</td>
<td>155</td>
<td>3</td>
<td>8</td>
<td>8</td>
<td>126.94</td>
<td>8 857.49</td>
</tr>
<tr>
<td>Urban Dictionary</td>
<td>244</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>51.01</td>
<td>54 441.56</td>
</tr>
<tr>
<td>Password dumps</td>
<td>815</td>
<td>0</td>
<td>44</td>
<td>3</td>
<td>199.20</td>
<td>39 155.22</td>
</tr>
<tr>
<td>Industry lists</td>
<td>876</td>
<td>0</td>
<td>32</td>
<td>3</td>
<td>364.91</td>
<td>37 096.71</td>
</tr>
<tr>
<td>Facebook names</td>
<td>364</td>
<td>0</td>
<td>23</td>
<td>4</td>
<td>107.78</td>
<td>14 425.13</td>
</tr>
<tr>
<td>BitSig</td>
<td>235</td>
<td>0</td>
<td>71</td>
<td>8</td>
<td>1 586.78</td>
<td>6 3818.81</td>
</tr>
<tr>
<td>Bitcoin IRC</td>
<td>454</td>
<td>1</td>
<td>17</td>
<td>6</td>
<td>777.52</td>
<td>25 355.79</td>
</tr>
<tr>
<td>Reddit</td>
<td>843</td>
<td>8</td>
<td>120</td>
<td>3</td>
<td>2 175.42</td>
<td>99 089.43</td>
</tr>
<tr>
<td>WikiQuote</td>
<td>281</td>
<td>0</td>
<td>3</td>
<td>7</td>
<td>113.60</td>
<td>17 700.88</td>
</tr>
<tr>
<td>BrainyQuote</td>
<td>61</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>85.12</td>
<td>14 037.94</td>
</tr>
<tr>
<td>Wiki/Brainy</td>
<td>83</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>101.05</td>
<td>14 481.48</td>
</tr>
<tr>
<td>Lyrics</td>
<td>438</td>
<td>0</td>
<td>17</td>
<td>4</td>
<td>270.28</td>
<td>19 257.41</td>
</tr>
<tr>
<td>Wikipedia</td>
<td>176</td>
<td>0</td>
<td>5</td>
<td>6</td>
<td>565.77</td>
<td>15 645.48</td>
</tr>
<tr>
<td>Openwall</td>
<td>456</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>60.69</td>
<td>14 097.56</td>
</tr>
<tr>
<td>Purdue</td>
<td>424</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>118.95</td>
<td>14 983.66</td>
</tr>
<tr>
<td>Keyboard Patterns</td>
<td>19</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>0.96</td>
<td>246.96</td>
</tr>
<tr>
<td>Non-word lists</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brute Force</td>
<td>586</td>
<td>2</td>
<td>84</td>
<td>2</td>
<td>96.44</td>
<td>23 796.09</td>
</tr>
<tr>
<td>Misc</td>
<td>268</td>
<td>7</td>
<td>268</td>
<td>1</td>
<td>73.67</td>
<td>26 941.39</td>
</tr>
<tr>
<td>Overall</td>
<td>1 730</td>
<td>21</td>
<td>488</td>
<td>3</td>
<td>2 846.23</td>
<td>260 792.30</td>
</tr>
</tbody>
</table>
Brain Wallet Usage

- 1,730 distinct brain wallets
- 1,686 passwords and passphrases
- 2,846 BTC (approximately 261K USD)

Notable Passwords/Phrases:

- This string contains 0.25 BTC hiding in plain sight.
- “”
- how much wood could a woodchuck chuck if a woodchuck could chuck wood
New Brain Wallet Usage by Month

New wallet value (USD)

uncompressed
compressed
Brain Drain Time

CDF: Time–to–Drain by Wallet Value

Overall
<=$0.01
<=$0.001

Hours to Drain

$P(TTD) \leq x$ hours
Draining: Passphrases vs. Passwords

Time to Drain by Password Length

Time to Drain by Password List
Chapter 6 Conclusions

- Developed methodology for measuring the use of brain wallets and their subsequent drains.
- Tested 3.9 trillion candidate passwords and passphrases.
- Found 1,730 brain wallets using 1,686 different passwords which have received 2,846 BTC (approx. $261K).
- Nearly all drained, many within seconds.
Chapter 6 Conclusions

“DO NOT USE BRAINWALLETS”
Chapter 6 Conclusions

“DO NOT USE BRAINWALLETS”

https://en.bitcoin.it/w/index.php?
  title=Brainwallet&oldid=61264

Now... with Science!
Thesis Contributions and Talk Outline

- Thesis: We **measure** cybercrime activity in the Bitcoin ecosystem to **better understand** attacker motivation and efficacy of various crimes and countermeasures.
  - Ch. 2 - Bitcoin Primer (covered in proposal)
  - Research Questions (covered in proposal)
  - Ch. 3 - Measuring Denial-of-Service Attacks in the Bitcoin Ecosystem (covered in proposal)
  - Ch. 4 - Measuring the Profits of Bitcoin Scams (covered in proposal)
  - Ch. 5 - Measuring the Supply and Demand for Bitcoin Scams (new)
  - Ch. 6 - Measuring the Use and Abuse of Brain Wallets (new)
  - Ch. 7 - Conclusions
Thesis Contributions

• Thesis: We measure cybercrime activity in the Bitcoin ecosystem to better understand attacker motivation and efficacy of various crimes and countermeasures.

• DDoS attack prevalence and impact

• Bitcoin scam prevalence and profit

• Brain wallet prevalence and drainer profit
Thanks!
Questions?