

# Empirical Analysis of Denial of Service Attacks in the Bitcoin Ecosystem

Marie Vasek   Micah Thornton   Tyler Moore

Computer Science & Engineering, Southern Methodist University, USA,  
mathornton@smu.edu

1st Workshop on Bitcoin Research  
Barbados  
March 7, 2014

# Reports of DDoS attacks are rampant

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?





slushcz

@slushcz

 Follow

slush's [#bitcoin](#) pool become a target of large DDoS. Please retweet new mining URL: [api3.bitcoin.cz:8332](#) as website is down at this moment.

 Reply  Retweet  Favorite  More

RETWEETS

4

FAVORITE

1

B



bitcoin



4:29 PM - 12 Oct 2011

# It's been an epic few days: What happened?

TOKYO - JAPAN - April 04, 2013

Dear Mt.Gox users and Bitcoiners,

It's been an epic few days on Bitcoin, with prices going up as high as \$142 per BTC. We all hope that this is just the beginning!

However, there are many who will try to take advantage of the system. The past few days were a reminder of this sad truth.

Mt.Gox has been suffering from its worst trading lag ever, 502 errors, and at one point some users were not able to log in their account. The culprit is a major DDoS attack against Mt.Gox.

Since yesterday, we are continuing to experience a DDoS attack like we have never seen. While we are being protected by companies like Prolexic, the sheer volume of this DDoS left us scrambling to fine-tune the system every few hours to make sure that things don't go beyond a few 502 error pages and trading lag.

# SatoshiDice hit by DDoS attack, but bets continue

Danny Bradbury (@dannybradbury) | Published on September 6, 2013 at 11:50 GMT | Bitcoin Gambling, Companies, News

# Bitcoin exchanges hit by DDoS attacks

By Tim Hornyak, IDG News Service

Feb 11, 2014 9:00 PM



The problems plaguing Bitcoin worsened Tuesday as online attacks on the digital currency's software affected two more exchanges.

**Major Bitcoin exchange Bitstamp has suspended bitcoin withdrawals amid distributed denial-of-service (DDoS) attacks.**

Last week, Mt. Gox, another big exchange, suspended bitcoin transfers from wallets it holds to external bitcoin addresses, as it had noted that a bug in the Bitcoin software could allow fraud.

The attack uses "transaction malleability to temporarily disrupt balance checking," Slovenia-based Bitstamp said on its [website](#), adding that no funds have been lost and that it's confident that transactions will be back to normal soon.

# Bitcoin Hit By 'Massive' DDoS Attack As Tensions Rise



[+ Comment Now](#) [+ Follow Comments](#)

A “massive” distributed denial of service (DDoS) attack is hitting [Bitcoin](#), according to trading venues, in what has been a tense week over alleged flaws in the various systems run by the virtual currency and its exchanges.

The attack picks on the very area – transaction malleability, or the potential renaming of transaction messages – that has become a bone of contention between different venues, and is blocking some transactions from being confirmed. The source of and reason for the attack have not been disclosed.

The value of Bitcoins has fallen dramatically in recent days. Earlier this week, Japanese exchange Mt Gox stopped trading, blaming transaction malleability issues in Bitcoin’s systems that purportedly allow traders to pretend a withdrawal has not gone through, and to receive the currency a second time.

# Motivation

- DDoS attacks are perhaps the most common scourge to afflict Bitcoin participants
- No one has systematically tracked DDoS on Bitcoin
- Thus it is hard to assess their impact on the Bitcoin ecosystem
- We measure DDoS reports to identify their real prevalence and impact



# Outline of today's talk

## 1 Methodology

- Data Collection
- Identifying Reported DDoS Attacks

## 2 Empirical Analysis

- Reported DDoS over Time and by Target
- DDoS Attacks on Mining Pools
- DDoS Attacks on Currency Exchanges

## 3 Conclusion

- Takeaways
- Future Work
- Questions?

# Outline

## 1 Methodology

- Data Collection
- Identifying Reported DDoS Attacks




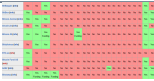
## 2 Empirical Analysis

- Reported DDoS over Time and by Target
- DDoS Attacks on Mining Pools
- DDoS Attacks on Currency Exchanges

## 3 Conclusion

- Takeaways
- Future Work
- Questions?

# Data sources

Source	Data Collected	Description
Bitcointalk.org		Forum posts containing "DDoS"
Bitcoincharts.org		Currency exchange information
Blockchain.info/pools  (Internet Archive)		Pool's historical hashrates
Bitcoin.it/wiki/Trade		List of services and pools



## A hora dos Bancos chegou.

September 11, 2011, 10:13:30 PM

#1

Primeiro, o monopólio de distribuição dos serviços postais foi duramente atingido pela Internet quando as pessoas descobriram que não precisavam mais comprar selos. Então, o monopólio da indústria do copyright foi categoricamente e sem a menor cerimônia atropelado pelos torrents. A terceira vítima e relativamente recente, é o antigo jornalismo centralizado com o seu apertado controle sobre a distribuição da informação sendo esculachado pela mídia alternativa. Como quarta e próxima vítima, há uma distribuição que poucas pessoas têm pensado em termos de informação: o dinheiro em nossa sociedade.

<http://www.bitcoinrevolution.com.br/a-hora-dos-bancos-chegou/>

30GH/s ANTMINER S1 *Classical mining rig by the trustworthy vendor* BITMAIN

Advertised sites are not endorsed by the Bitcoin Forum. They may be unsafe, untrustworthy, or illegal in your jurisdiction. [Advertise here.](#)



## Re: A hora dos Bancos chegou.

September 12, 2011, 12:05:27 AM

#2

Quote from: jatajuta on September 11, 2011, 10:13:30 PM

Primeiro, o monopólio de distribuição dos serviços postais foi duramente atingido pela Internet quando as pessoas descobriram que não precisavam mais comprar selos. Então, o monopólio da indústria do copyright foi categoricamente e sem a menor cerimônia atropelado pelos torrents. A terceira vítima e relativamente recente, é o antigo jornalismo centralizado com o seu apertado controle sobre a distribuição da informação sendo esculachado pela mídia alternativa. Como quarta e próxima vítima, há uma distribuição que poucas pessoas têm pensado em termos de informação: o dinheiro em nossa sociedade.



## favorite dos game?

February 28, 2014, 05:42:34 AM

Just wondering what everyone's favorite old school dos games are i'm pretty partial to duke3d one of the best games ever lol.

BitcoinRoll.org 0.995 House Edge, Instant,

included in a block to be properly completed. When you send a transaction, it is broadcast to miners. Miners can then optionally include it in their next block inclined to include your transaction if it has a transaction fee.

Advertised sites are not endorsed by the Bitcoin Forum. They may be unsafe, untrustworthy, or illegal in your jurisdiction. [Advertise here.](#)



## Re: favorite dos game?

February 28, 2014, 06:15:39 AM

**Quote from: cybershawrk on February 28, 2014, 05:42:34 AM**

Just wondering what everyone's favorite old school dos games are i'm pretty partial to duke3d one of the best games ever lol.

Civilization and Doom.

◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡

# From posts to attacks

- Google API searched on Bitcointalk.org found **2940 pages** mentioning "DDoS"
- Pages were pared down to **1355 distinct threads (first page only)**
- Rule based classifier flagged **362 posts** as likely attacks
  - Whitelist: "unreachable", "offline", "on-line", "down", "flooding", "attack", "ddos", "unavailable", "blocking" and "connect"
  - Blacklist: "anti-ddos" or "vote"
  - Flagged posts contain at least one word in the whitelist and none in the blacklist
- Manual inspection of posts yields **200 attacks**
- De-duplication yields **142 distinct attack reports**

# Outline

## 1 Methodology

- Data Collection
- Identifying Reported DDoS Attacks

## 2 Empirical Analysis

- Reported DDoS over Time and by Target
- DDoS Attacks on Mining Pools
- DDoS Attacks on Currency Exchanges

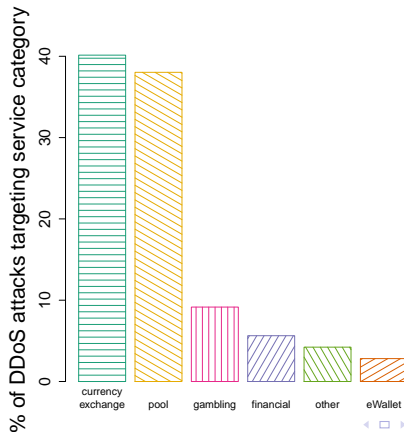
## 3 Conclusion

- Takeaways
- Future Work
- Questions?

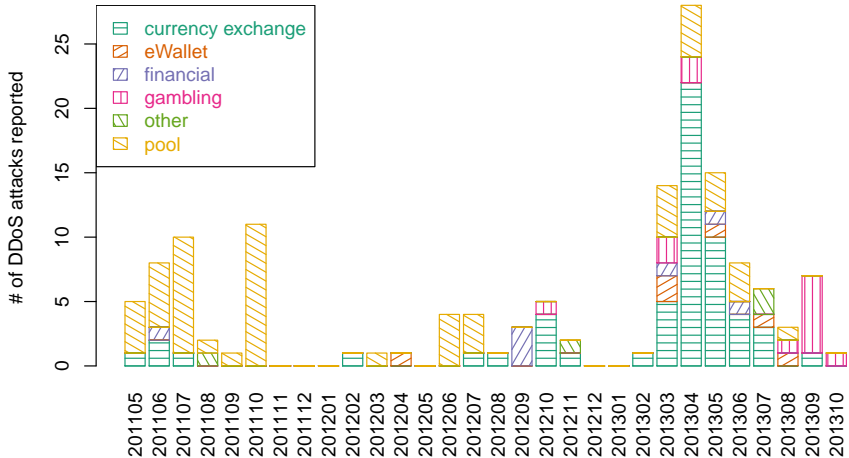


# Mapping attacks to Bitcoin services

- Examined **1 240 services** including **32 mining pools**
- **142 distinct DDoS attacks** reported
- **46 specific services** were targeted:



# Reported DDoS over time and by category



# Identifying the use of anti-DDoS mechanisms

- Anti-DDoS mechanisms include content distribution networks (CDNs) and clever firewalls
- Anti-DDoS services identified: **Amazon, Cloudflare, Incapsula**
- Resolved the IP addresses of Bitcoin services and compared with known CDN IP ranges
- Found **178 services** that used Anti-DDoS countermeasures out of a total **1190 services**

# DDoS attacks and countermeasures by service category

Category	#	Suffer DDoS		Use Anti-DDoS	
		%	Sig.?	%	Sig.?
<i>Average</i>		7.3		19.9	
Currency exchanges	119	<b>10.9</b>	+	<b>36.1</b>	+
Financial	26	<b>15.4</b>	+	26.9	
Pool	41	<b>28.6</b>	+	<b>34.1</b>	+
Bitcoin eWallets	17	<b>26.8</b>	+	35.3	
Bitcoin payment systems	11	9.1		18.2	
Material/physical products	295	<b>0.7</b>	–	<b>10.5</b>	–
Internet & mobile services	225	1.8		16.9	
Online products	185	3.8		14.6	
Professional services	137	0		10.2	
Travel/tourism/leisure	78	0		10.3	
Commerce & community	71	1.4		12.7	
Getting started	31	0		12.9	

# Do DDoSed firms buy anti-DDoS protection?

- Does suffering a DDoS attack make a service more likely to purchase DDoS countermeasures?

	Use Anti-DDoS		No Anti-DDoS	
	#	%	#	%
Suffered DDoS	25	54%	21	46%
No DDoS	178	15%	1 012	85%

# Do DDoSed firms buy anti-DDoS protection?

- Does suffering a DDoS attack make a service more likely to purchase DDoS countermeasures? **Yes!**

	Use Anti-DDoS		No Anti-DDoS	
	#	%	#	%
Suffered DDoS	25	54%	21	46%
No DDoS	178	15%	1 012	85%

# DDoS attacks on mining pools

- Does the size of a mining pool affect its tendency to be DDoSed?
- Captured 22 historical records of hashrate shares of mining pools
- A pool is “big” if it has at least a 5% share of the hash rate during 2 or more observations

	Small Pools		Big Pools	
	#	%	#	%
Suffered DDoS	7	17.1%	5	62.5%
No DDoS	34	82.9%	3	37.5%

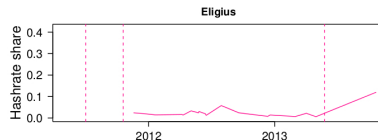
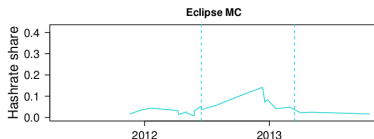
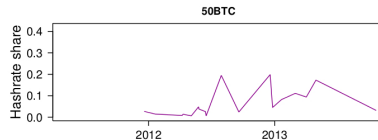
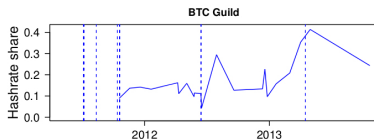
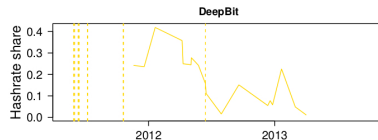
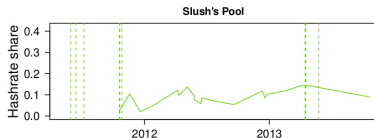
# DDoS attacks on mining pools

- Does the size of a mining pool affect its tendency to be DDoSed? **Yes!**
- Captured 22 historical records of hashrate shares of mining pools
- A pool is “big” if it has at least a 5% share of the hash rate during 2 or more observations

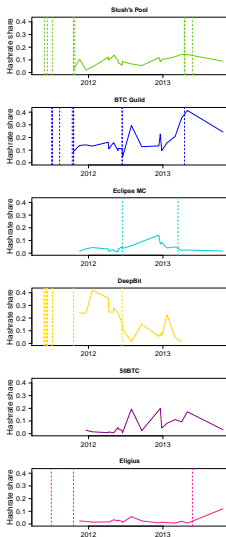
	Small Pools		Big Pools	
	#	%	#	%
Suffered DDoS	7	17.1%	5	62.5%
No DDoS	34	82.9%	3	37.5%



# Historical hash-rate-based market shares

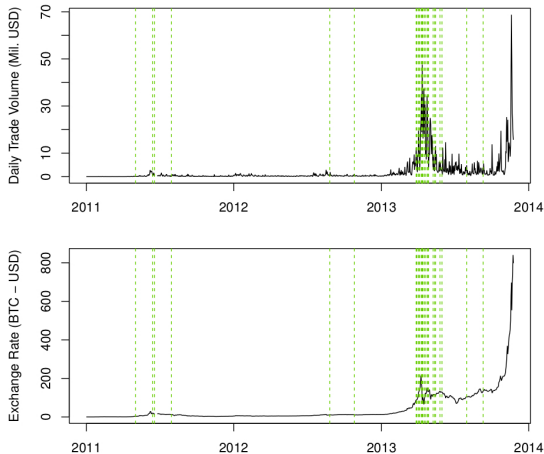


# Historical hash-rate-based market shares



- Pools sometime unfazed by DDoS attacks
  - BTC Guild increased its market share after an attack in mid-2012
  - But its share decreased after an attack in mid-2013
- DDoS attacks sometimes target multiple pools at once
  - Deepbit, BTC Guild, and Eclipse targeted at the same time as seen mid-2012
- We can reject the notion that DDoS attacks always trigger decline in market share
- DDoS attacks often precede shake ups in pool marketshare

# DDoS effects on trade volume and price (Mt. Gox)



# DDoS effects on trade volume and price (Mt. Gox)

- **29 total attacks** reported on Mt. Gox
- We compare transaction volume 1 week prior to DDoS and 1 week after DDoS

$\Delta$ Transaction Vol.	# of Attacks	% Attacks	% Change
Increase	12	41.4%	68.1%
Decrease	17	58.6%	31.9%

- Fall in transaction volume more common than rise after DDoS
- When increases in transaction volume do occur, the magnitude of change is greater than for decreases

# Outline

## 1 Methodology

- Data Collection
- Identifying Reported DDoS Attacks

## 2 Empirical Analysis

- Reported DDoS over Time and by Target
- DDoS Attacks on Mining Pools
- DDoS Attacks on Currency Exchanges

## 3 Conclusion

- Takeaways
- Future Work
- Questions?

# Takeaways

- 7% of all known operators have been subject to DDoS attacks
- Currency exchanges, mining pools, gambling operators, eWallets, and financial services are more likely to be attacked
- Services that are attacked are more than 3 times as likely to buy anti-DDoS services
- Large mining pools more likely to be DDoSed than small pools

# Future work

- Get a more accurate, network-based measure of Bitcoin DDoS
- Explore the relationship between DDoS and other currencies (e.g., Litecoin)
- Measure other anti-DDoS services
- Study impact of other factors on DDoS attacks (e.g., mining pool structure)

# Questions?