Booted: An Analysis of a Payment Intervention on a DDoS-for-Hire Service

Ryan Brunt, Prakhar Pandey, Damon McCoy

NYU
TANDON

Introduction: Booters

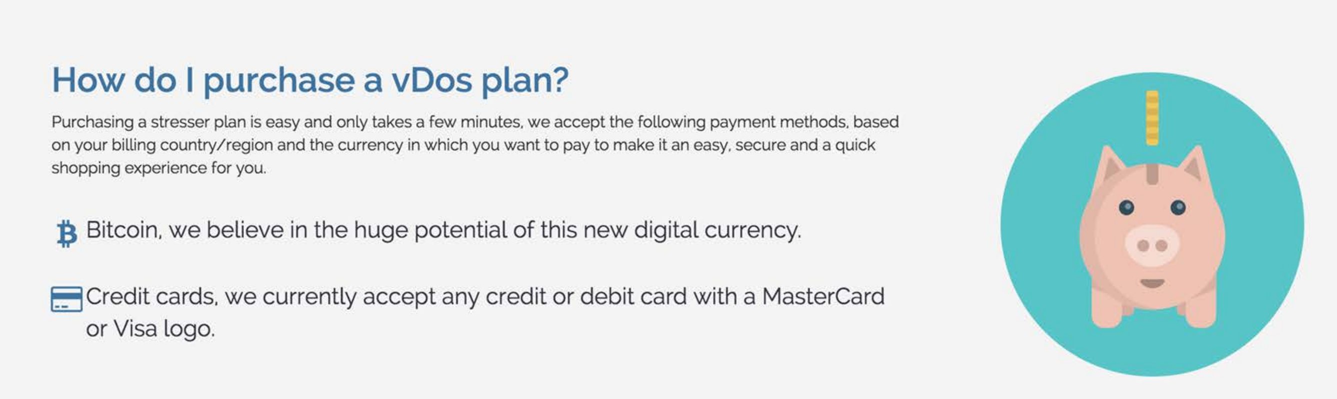
DDoS-for-hire, cheap way to launch attacks ($5)

Front as legitimate stress testers, but advertise on hacker forums

Went unchecked for a number of years until researchers, payment processors, and law enforcement took an interest

Intervention: PayPal ramped up detection of booter accounts

Our goal was to perform a quantitative analysis of the impact using leaked data

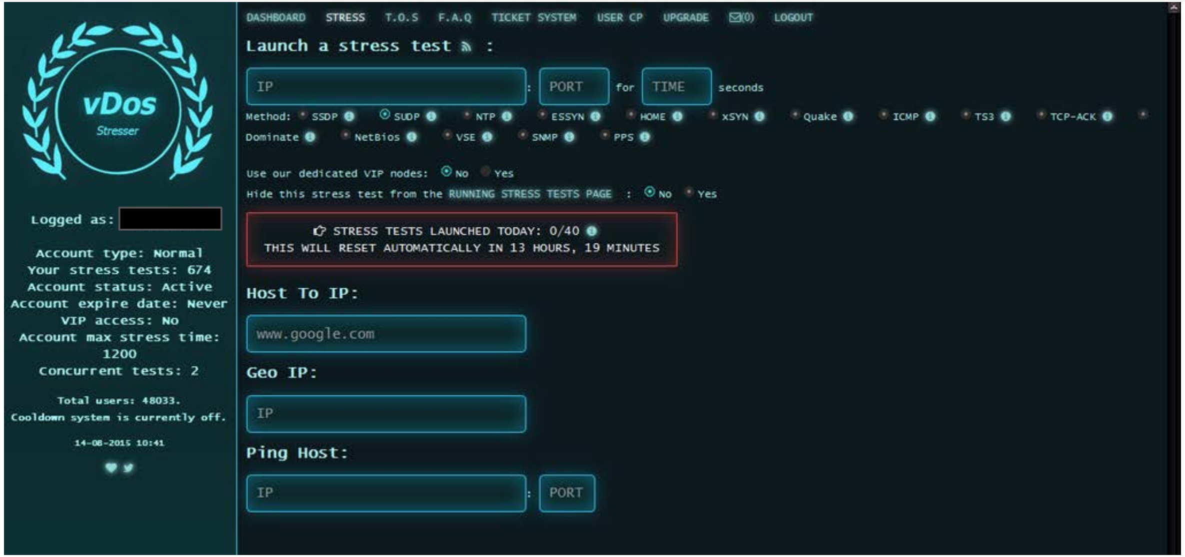


How do I purchase a vDos plan?

Purchasing a stresser plan is easy and only takes a few minutes, we accept the following payment methods, based on your billing country/region and the currency in which you want to pay to make it an easy, secure and a quick shopping experience for you.

₿ Bitcoin, we believe in the huge potential of this new digital currency.

💳 Credit cards, we currently accept any credit or debit card with a MasterCard or Visa logo.



Launch a stress test :

IP : PORT for TIME seconds

Method: ○ SSDP ● SUDP ○ NTP ○ ESSYN ○ HOME ○ xSYN ○ Quake ○ ICMP ○ TS3 ○ TCP-ACK ○ Dominate ○ NetBios ○ VSE ○ SNMP ○ PPS

Use our dedicated VIP nodes: ● No ○ Yes

Hide this stress test from the RUNNING STRESS TESTS PAGE : ● No ○ Yes

STRESS TESTS LAUNCHED TODAY: 0/40
THIS WILL RESET AUTOMATICALLY IN 13 HOURS, 19 MINUTES

Host To IP:

www.google.com

Geo IP:

IP

Ping Host:

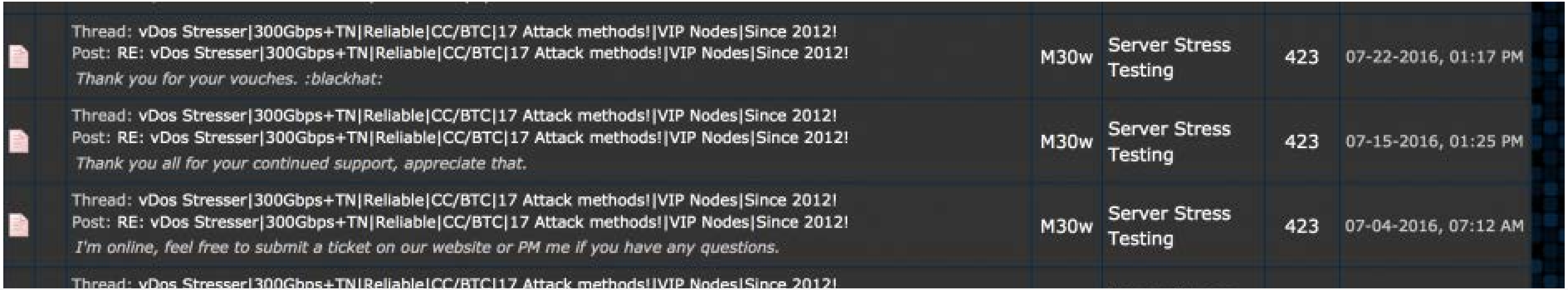
IP : PORT

Logged as: [redacted]

Account type: Normal
Your stress tests: 674
Account status: Active
Account expire date: Never
VIP access: No
Account max stress time: 1200
Concurrent tests: 2

Total users: 48033.
Cooldown system is currently off.

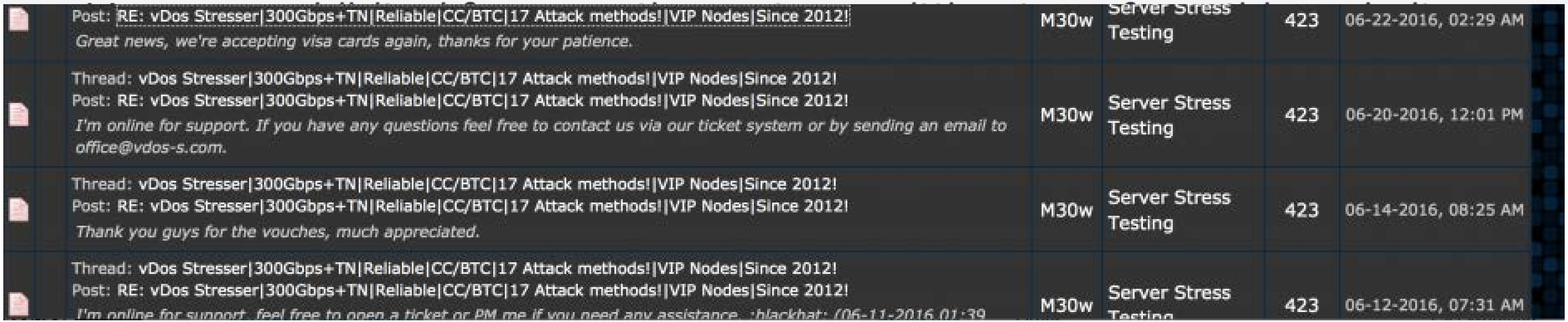
14-08-2015 10:41



Thread: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! Post: RE: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! *Thank you for your vouches. :blackhat:*	M30w	Server Stress Testing	423	07-22-2016, 01:17 PM
Thread: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! Post: RE: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! *Thank you all for your continued support, appreciate that.*	M30w	Server Stress Testing	423	07-15-2016, 01:25 PM
Thread: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! Post: RE: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! *I'm online, feel free to submit a ticket on our website or PM me if you have any questions.*	M30w	Server Stress Testing	423	07-04-2016, 07:12 AM
Thread: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012!				

11. VISITOR MATERIAL AND CONDUCT

11.1 You are prohibited from stressing internet connections and/or servers that You do not have ownership of or authorization to test.



Post: RE: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! *Great news, we're accepting visa cards again, thanks for your patience.*	M30w	Server Stress Testing	423	06-22-2016, 02:29 AM
Thread: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! Post: RE: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! *I'm online for support. If you have any questions feel free to contact us via our ticket system or by sending an email to office@vdos-s.com.*	M30w	Server Stress Testing	423	06-20-2016, 12:01 PM
Thread: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! Post: RE: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! *Thank you guys for the vouches, much appreciated.*	M30w	Server Stress Testing	423	06-14-2016, 08:25 AM
Thread: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! Post: RE: vDos Stresser|300Gbps+TN|Reliable|CC/BTC|17 Attack methods!|VIP Nodes|Since 2012! *I'm online for support, feel free to open a ticket or PM me if you need any assistance. :blackhat: (06-11-2016 01:39*	M30w	Server Stress Testing	423	06-12-2016, 07:31 AM

User: Does your booter support DoTA 2? …

Admin: We don’t have a DoTA2-Specific Attack method, … I’m quite sure that any DoTA 2 server you attack with vDos will go down …

User: … do you have any suggested attack method?

Admin: … I’d recommend trying SSDP or NTP

User: my account have been banned…

Admin: As of now, you have 8111 boots, I'm basically losing money by having you as a customer. I'm afraid I'd have to refund both of your payments …

Admin: We have received numerous reports that you are stress testing targets that you do not own. you are breaking our ToS

User: My account have been banned for sending out ddos? What else should I use this booter for?

Admin: We're a legitimate stress testing company, not a DDoS service...We are not going to refund your payment

Leaked Data

Backend database for vDoS website, HTTP Access Logs, scraped data from website

75,000 Registered users (10,000 with payment/attack); **$600,000 in revenue** over two years

270,000 Victims, **48 attack years**, 900,000 attacks over 12 months

Timeline

2014 - beginning of records in leaked vDoS DB

Summer 2015 - PayPal freezes a large portion of vDoS accounts

Between Sept - Oct 2015 PayPal no longer available to customers

July 2016 vDoS database leaked

Sept 2016 vDoS owners arrested

Validation: Table Agreement

22 tables but we limit our analysis to 6 tables

Validation of previous study accounts

Consistency between subscription info and payments

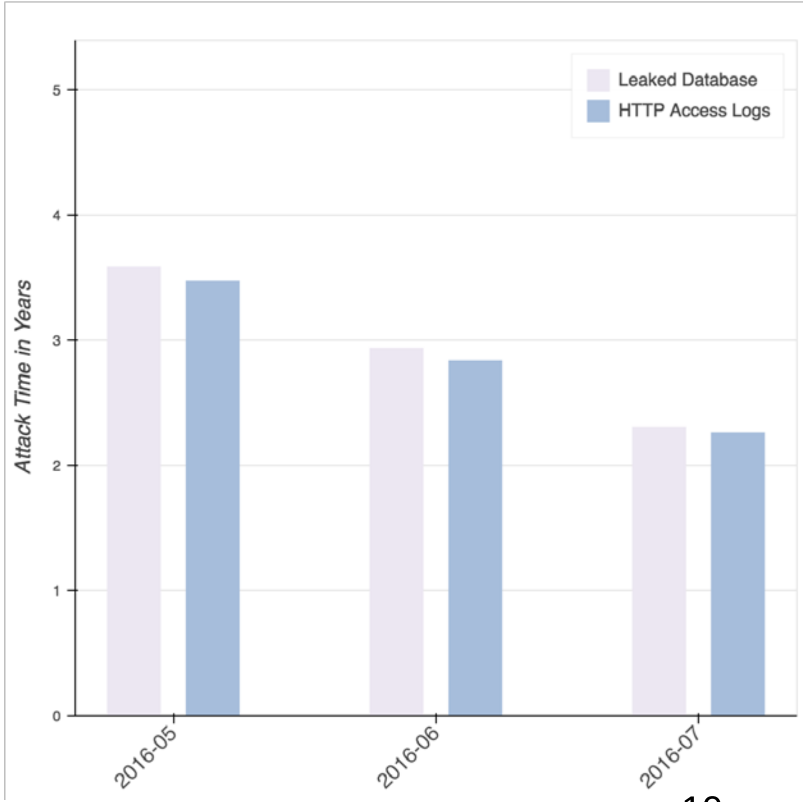
Validation: Attack Logs

Three sources of attack data

Http logs combined with scraped data provide the most complete picture

Deleted attack information on rolling basis in backend database (only 3 months)

Overlapping data matched up



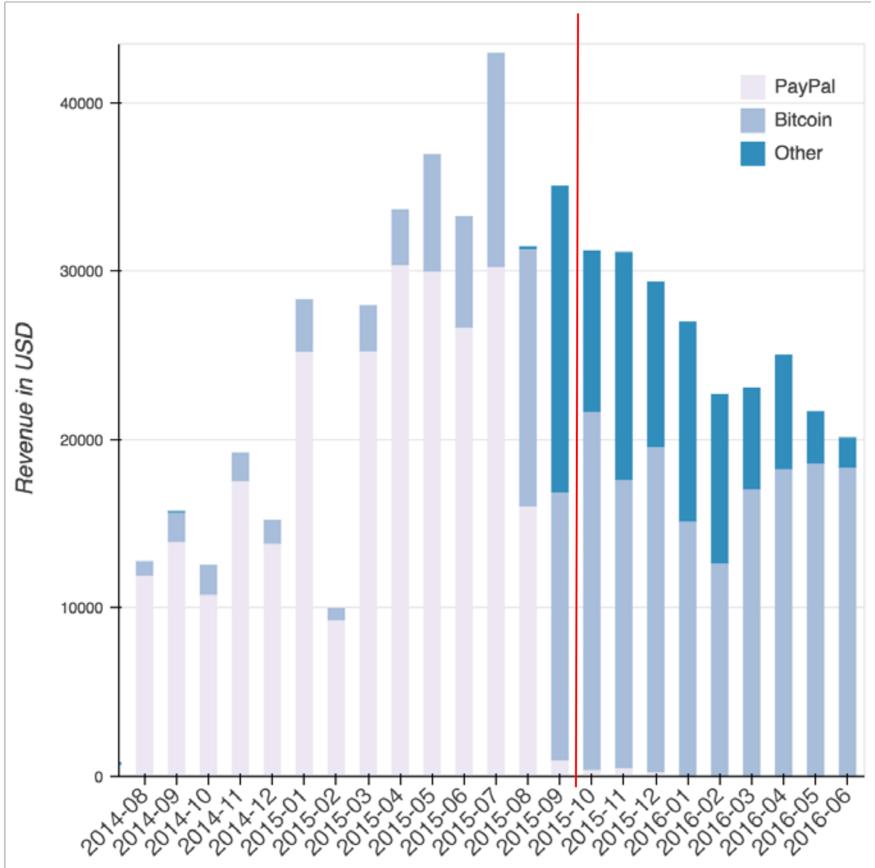
Validation: Bitcoin Transactions

Validated transactions in database were all confirmed on the blockchain

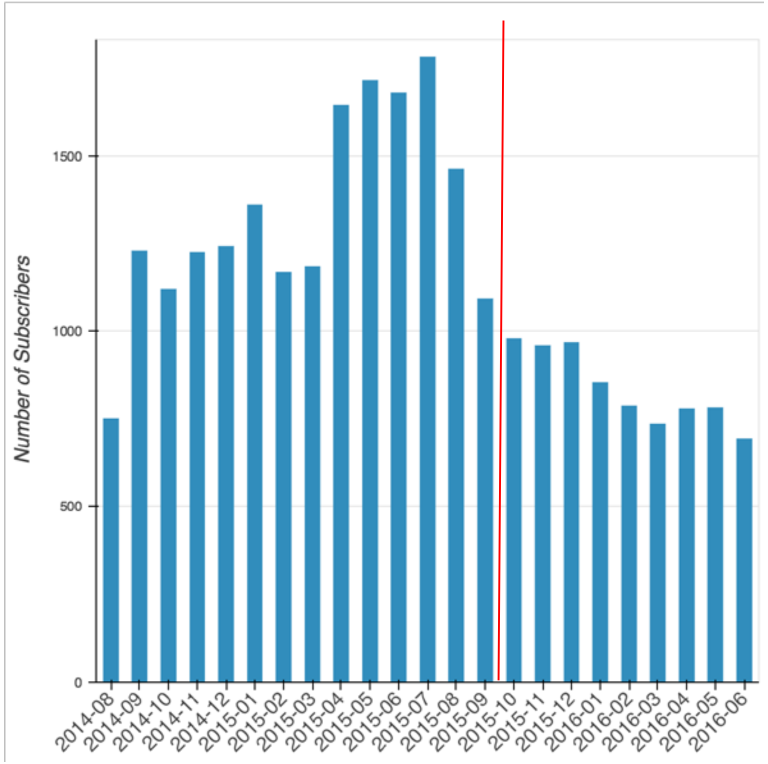
Validated txs at the address were recorded in database

Investigated blacklisting service estimated revenue at $375 (chump change)

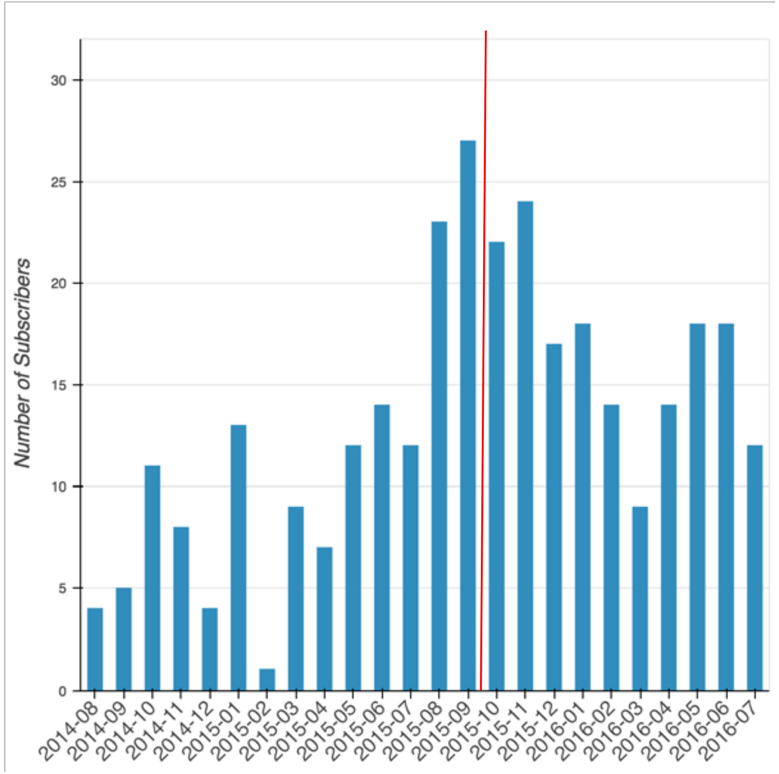
Analysis: Revenue



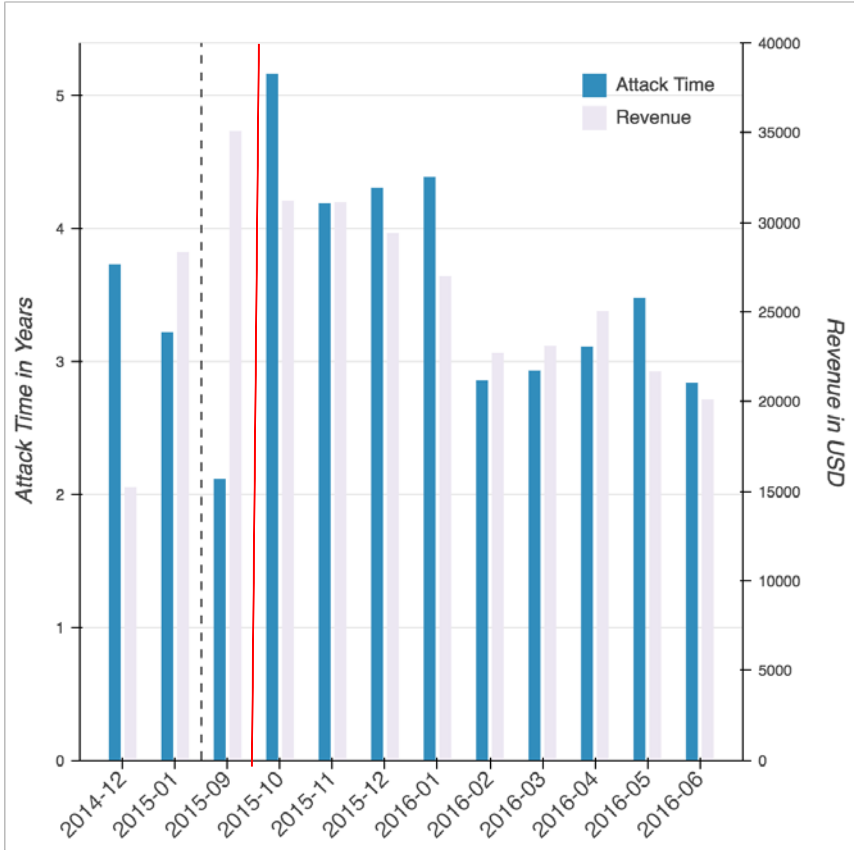
Analysis: Subscriber Behavior



Analysis: Subscriber Behavior



Analysis: Attacks



Analysis: Estimated Profit Margins

1 month of sent payments August 2015 - $10,000

$6,000 went to hosting and customer service.

Corresponding Revenue was $30,000

8 attack servers, 6 Customer service reps, etc. ~$12,000

Likely profitable still ($20,000 in revenue post intervention)

Discussion and Limitations

Case study

Insight into understanding the business and its customers

Doesn’t capture the ecosystem

Validates prior work

Conclusions

One possible explanation for decline BTC still difficult to use for average user

As Bitcoin becomes more commonplace it will be more difficult to intervene against criminal services

Booters cause a lot of harm, but it is possible to reduce the damage

Thank you!

Questions