Intervening in the market for DoS-for-hire services

Ben Collier

Co-authors: Daniel Thomas, Richard Clayton, Alice Hutchings, Ildiko Pete

Cambridge Cybercrime Centre

UNIVERSITY OF CAMBRIDGE

Contents

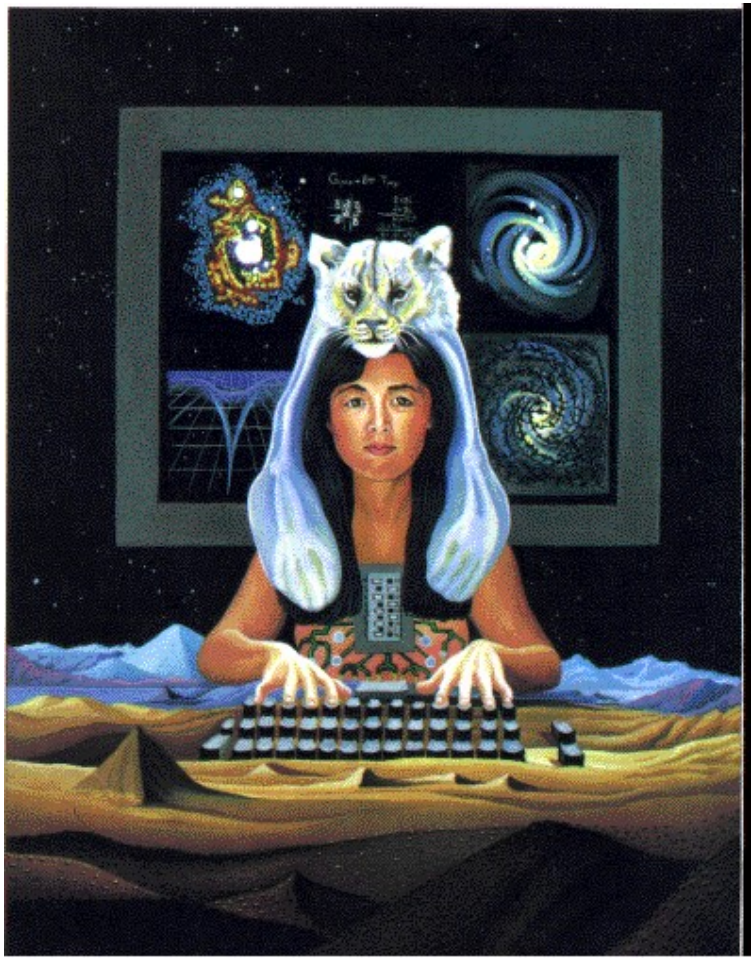
- Cybercrime and communities
- Booter services
- Law enforcement interventions in online criminal markets
- Quantitative analysis – how effective are different kinds of disruption?
- Qualitative analysis – why were they effective?
- Conclusions

Cybercrime and communities

- Much like traditional crime, community and networks are important
- Not just economic – norms, values and cultural factors
- Often around central sites such as cryptomarkets, IRC networks, chat channels and hacker forums
- These act as places where communities can form
- Communities
  - Human interactions, friendships, and connections
  - Share skills
  - Alternative site of social capital
  - Buy services

DDoS

- Knock targets offline – other Internet users, schools, businesses, infrastructure
- Uses a variety of methods to overwhelm target with too much traffic
- Any cybercriminals in the audience?



Google

? booter

All Images Videos Shopping News More Settings Tools

About 5 300 000 results (0,35 seconds)

StressThem.to - The next generation IP Stresser
https://www.stressthem.to/

StressThem is the strongest **Booter** on the market with a total capacity of 1000Gbit/s. Sign up and receive a free plan.
You've visited this page 4 times. Last visit: 6/10/19

DDoS for Hire | Booter, Stresser and DDoSer | Imperva
https://www.imperva.com/learn/application-security/booters-stressers-ddosers/

Booters, Stressers and DDoSers. ... Historically, DDoS attacks are associated with hacker and hacktivist groups and often considered to be a work of professional cyber crooks. ... The services offered are exactly the same, so there's no actual difference between **booter**, stresser, or ...
DDoS Attack Scripts · Botnet · DDoS attacks

Booter - Wikipedia
https://en.wikipedia.org/wiki/Booter

Booter may refer to: PC **booter**, software loaded directly at the bootup of a computer, without the help of an operating system; **Booter**, a tool for performing a ...

WebStresser - IP Stresser / Booter | DDoS Tool
https://webstresser.biz/

webstresser.biz is the strongest IP Stresser / **Booter** on the market, we provide strongest and most reliable server stress testing, with up to 950Gbps!

VIP Booter - The Cheapest Hard Hitting Lifetime Booter / IP Stresser ...
https://www.booter.vip/

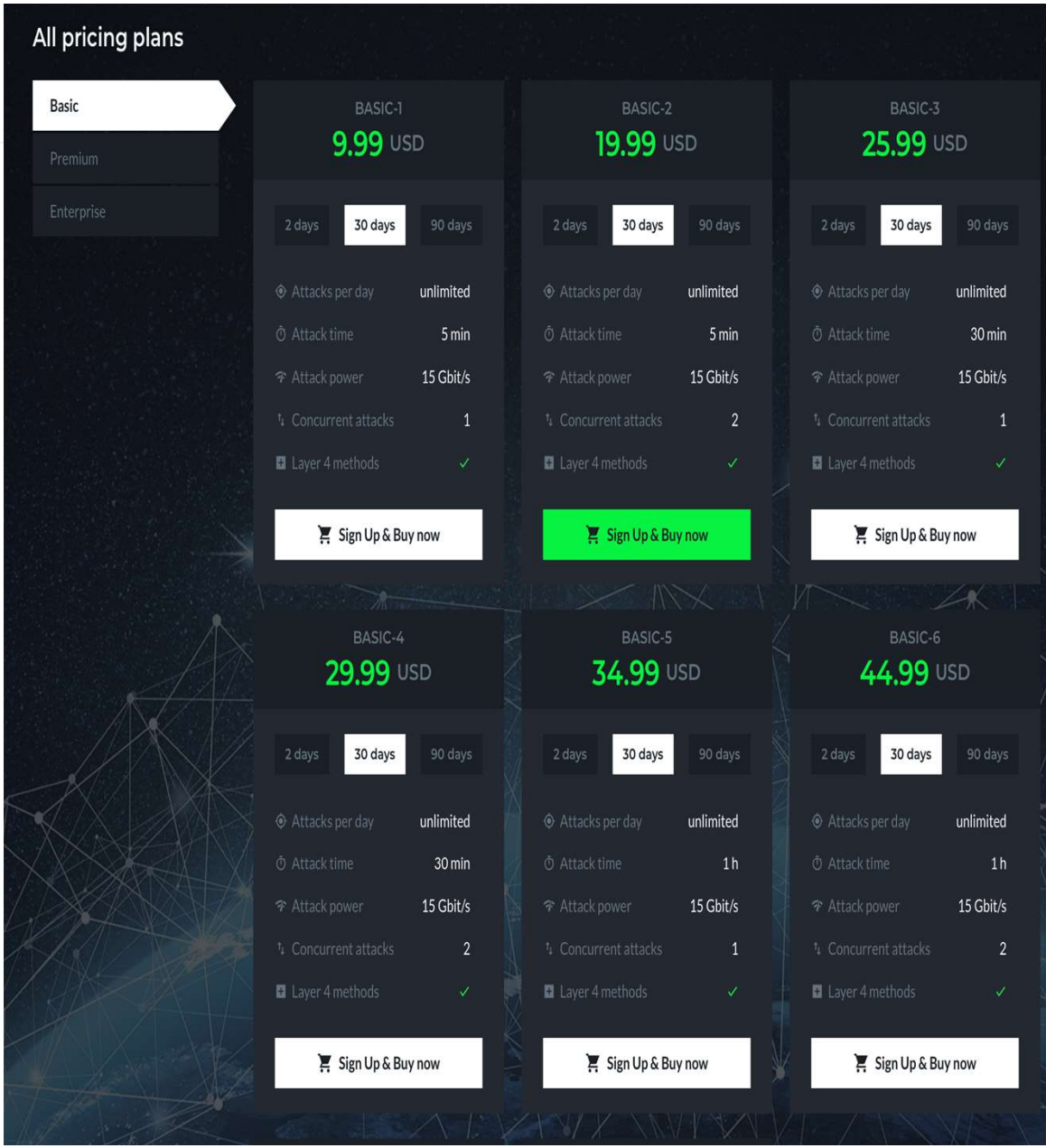
VIP **BOOTER** - **BOOTER**.VIP Worlds Best, Cheapest Most Powerful, The Strongest Hard Hitting IP Stresser / **Booter** for DDOS - 45 GBPS Downs Anything. Strong ...

XyZ Booter/Stresser - TOP 1 IP Stresser
https://www.booter.xyz/

XyZBooter LTD is the best **booter** / stresser / ip stresser in the market. We are kind of legal 'DDoS for Hire' company that provide online web panel which you ...

Booter.pw
https://booter.pw/

The website have been moved to http://ddosbooterndoyow.onion/auth/login We are working on a



Dashboard

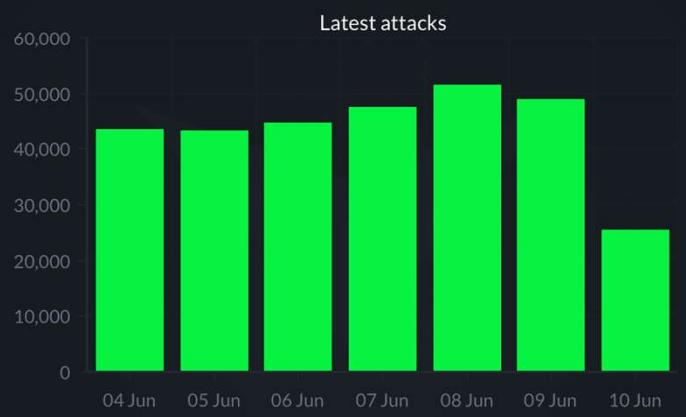
Welcome to our brand new dashboard, you will be able to find statistics and a general overview of your account here.

Upgrade

Network statistics

Attack statistics

Commonly used methods



Online users 122

Total users 397541

Running attacks 76

Total attacks 6394327

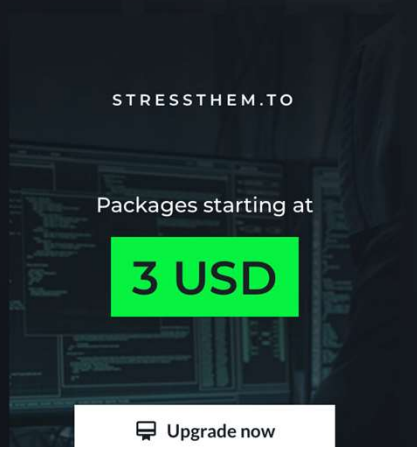
Account overview

Username	stresser12
2FA status	✕
Total balance	0.00 USD
Referred users	0
Referral link	https://www.stressthem.to/?ref=7L0TWFPE

Booter conditions

Active plan	Free Package
Expiration	lifetime
Max. boots per day	unlimited
Max. concurrent boots	1/1
Max. boot time	5 min
Boot power	1 Gbit/s

Upgrade now!



Recent News

Payments

Admin 17 May 2019, 12:33

Dear users,
Bitcoin payments are fully working again.

Kind Regards,
Your StressThem Team

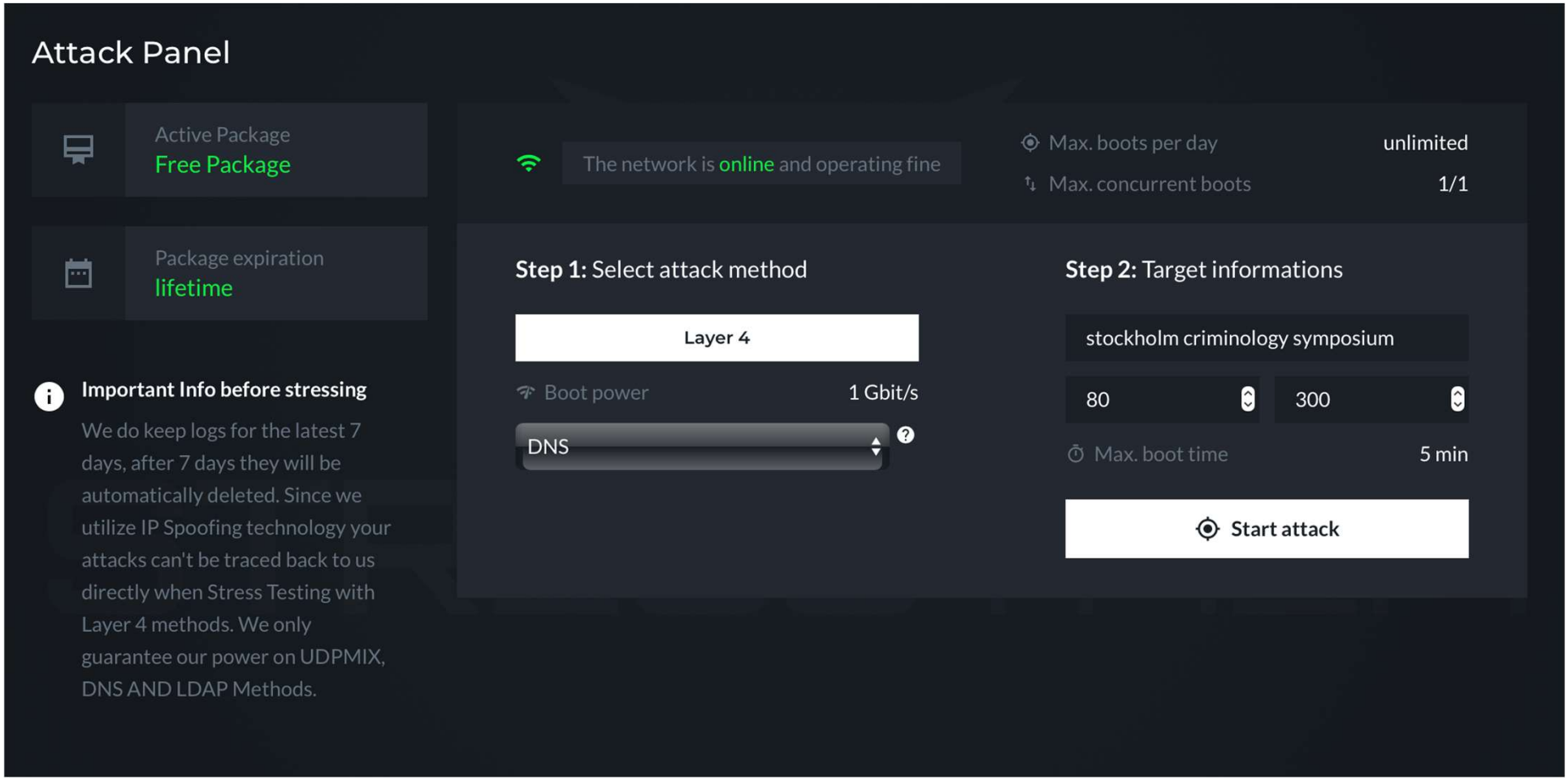
Power

Payments

Bitcoin payments are fully working again. Thanks for your patience.

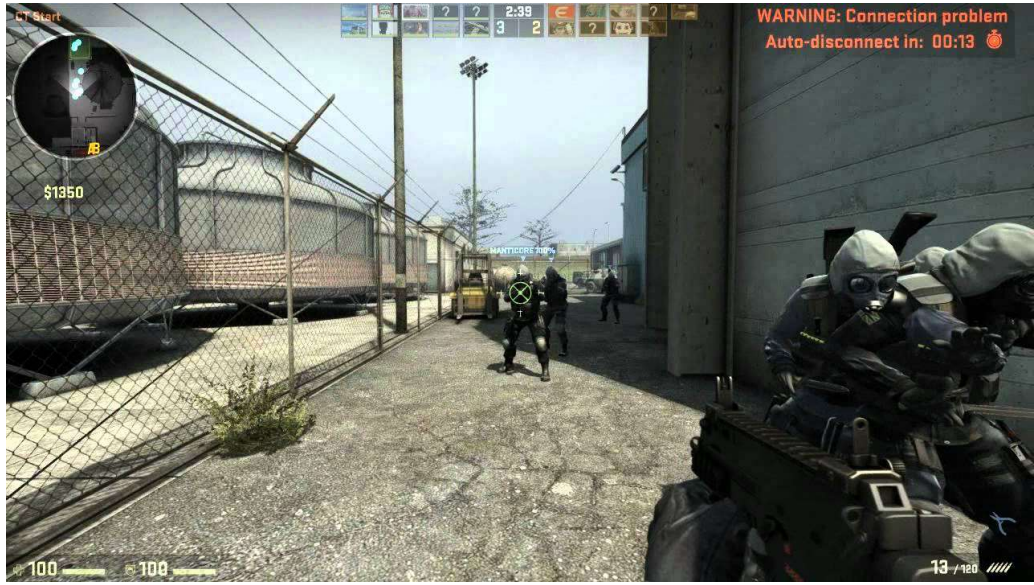
Network status

The network is online and operating fine


Attack Panel
Active Package
Free Package
Package expiration
lifetime
Important Info before stressing
We do keep logs for the latest 7 days, after 7 days they will be automatically deleted. Since we utilize IP Spoofing technology your attacks can't be traced back to us directly when Stress Testing with Layer 4 methods. We only guarantee our power on UDPMIX, DNS AND LDAP Methods.
The network is online and operating fine
Max. boots per day
unlimited
Max. concurrent boots
1/1
Step 1: Select attack method
Layer 4
Boot power
1 Gbit/s
DNS
Step 2: Target informations
stockholm criminology symposium
80
300
Max. boot time
5 min
Start attack

Booters

- First large-scale cyberattack market for completely unskilled users
- Providers set up infrastructure and then sell this attack capacity to users
- Buy attacks for $5 per month
- Usually targeted at gamers – troll culture
- Advertised through Youtube, Twitch, word-of-mouth, Discord channels and Google
- Originally centred around the Hackforums forum, but thrown off
- Now a dispersed set of microcommunities
- Low cultural capital – “skids”
- c. 50 internationally at any time, most resell capacity from the top ten



Interventions

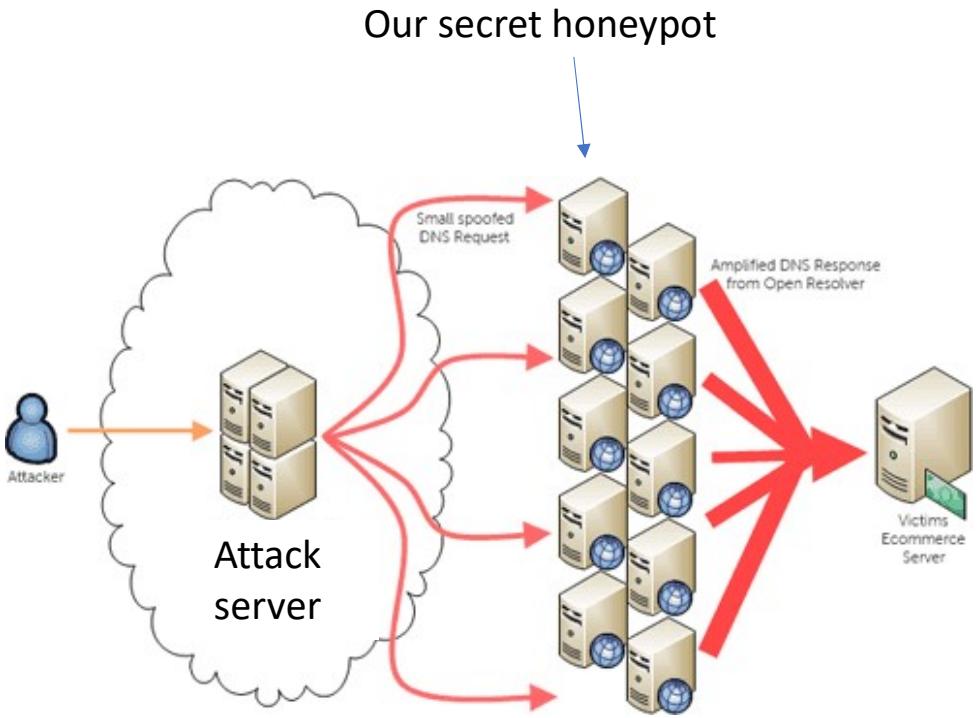
- Intervening in online criminal markets is challenging
- These tend to be highly resilient (e.g. cryptomarkets)
- High levels of displacement
- Crackdown policing causes its own harms and is limited in effect
- Still little understanding of best practice
- We considered four types of intervention:
  - Messaging
  - Sentencing
  - Takedowns
  - Arrests

Methods

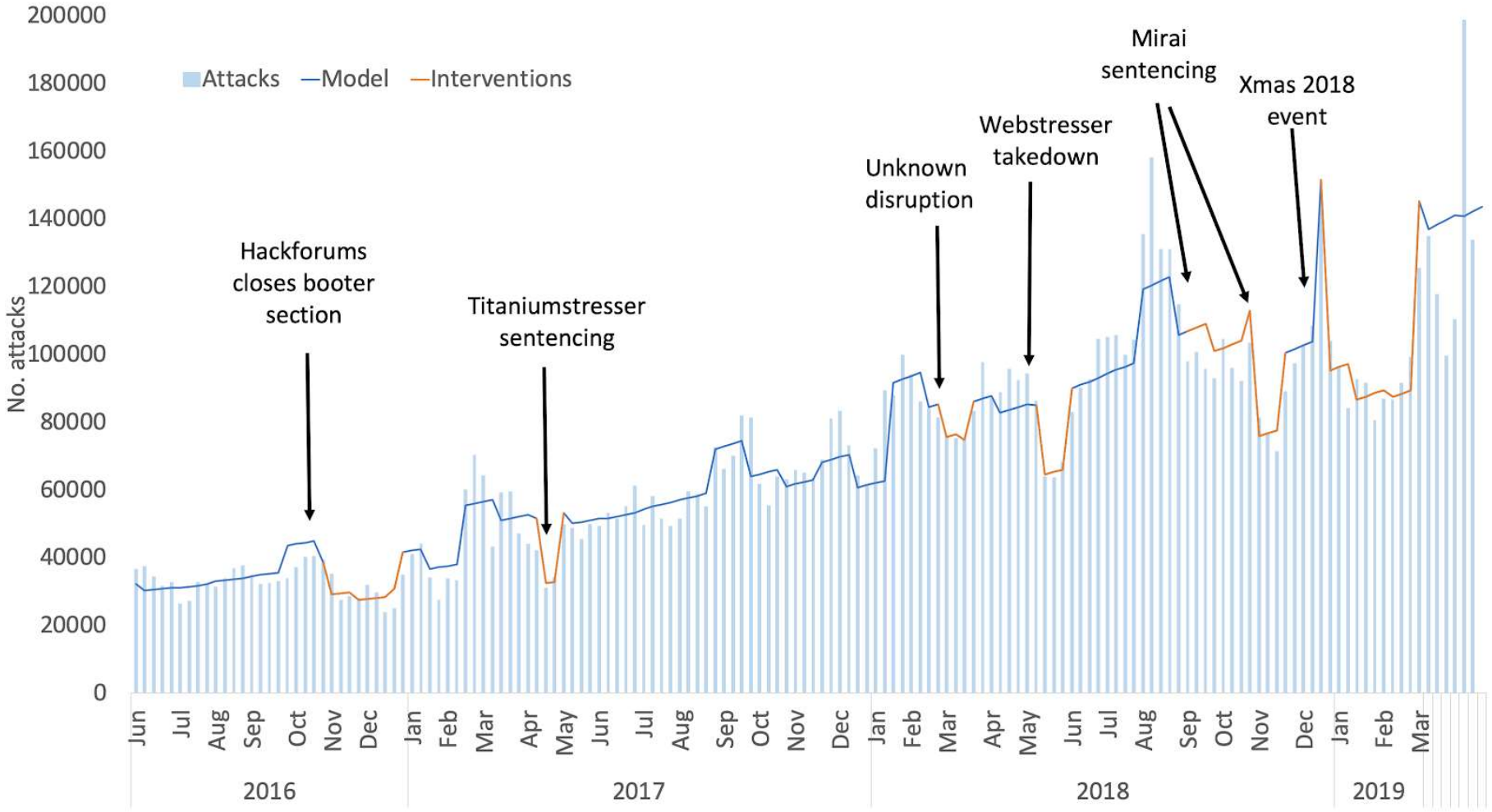
- Mixed-methods study
- Qualitative and quantitative approaches

Quantitative analysis

- Honeypots – measure of attacks
  - Booters use two methods of sourcing attack power – botnets and reflectors
  - We can pretend to be reflectors (so booters try to use us for attacks) and observe attacks in real time as they occur
- Self-reported attack data (includes botnet attacks)
- Negative binomial regression modelling to estimate effect sizes



Results – overall model

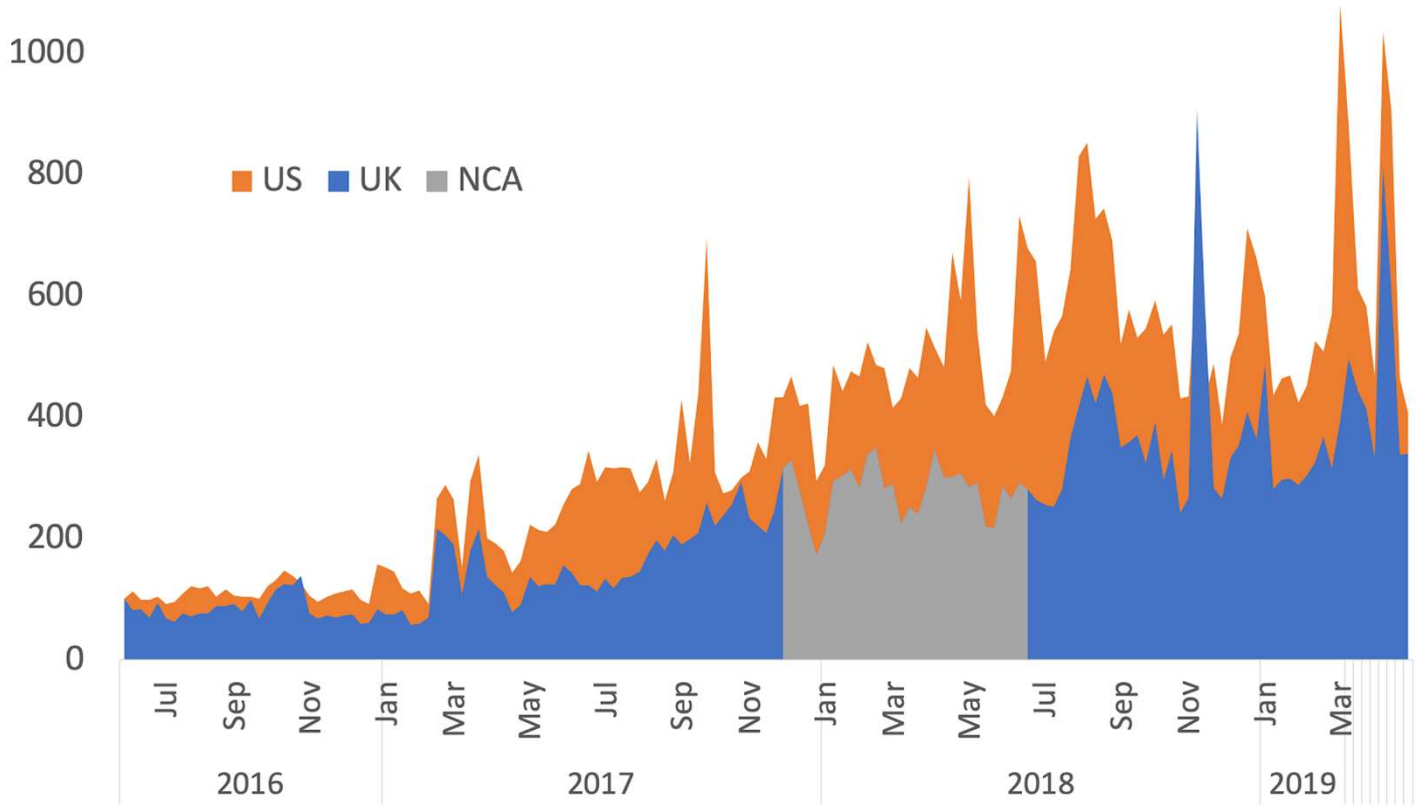


Estimated effect sizes

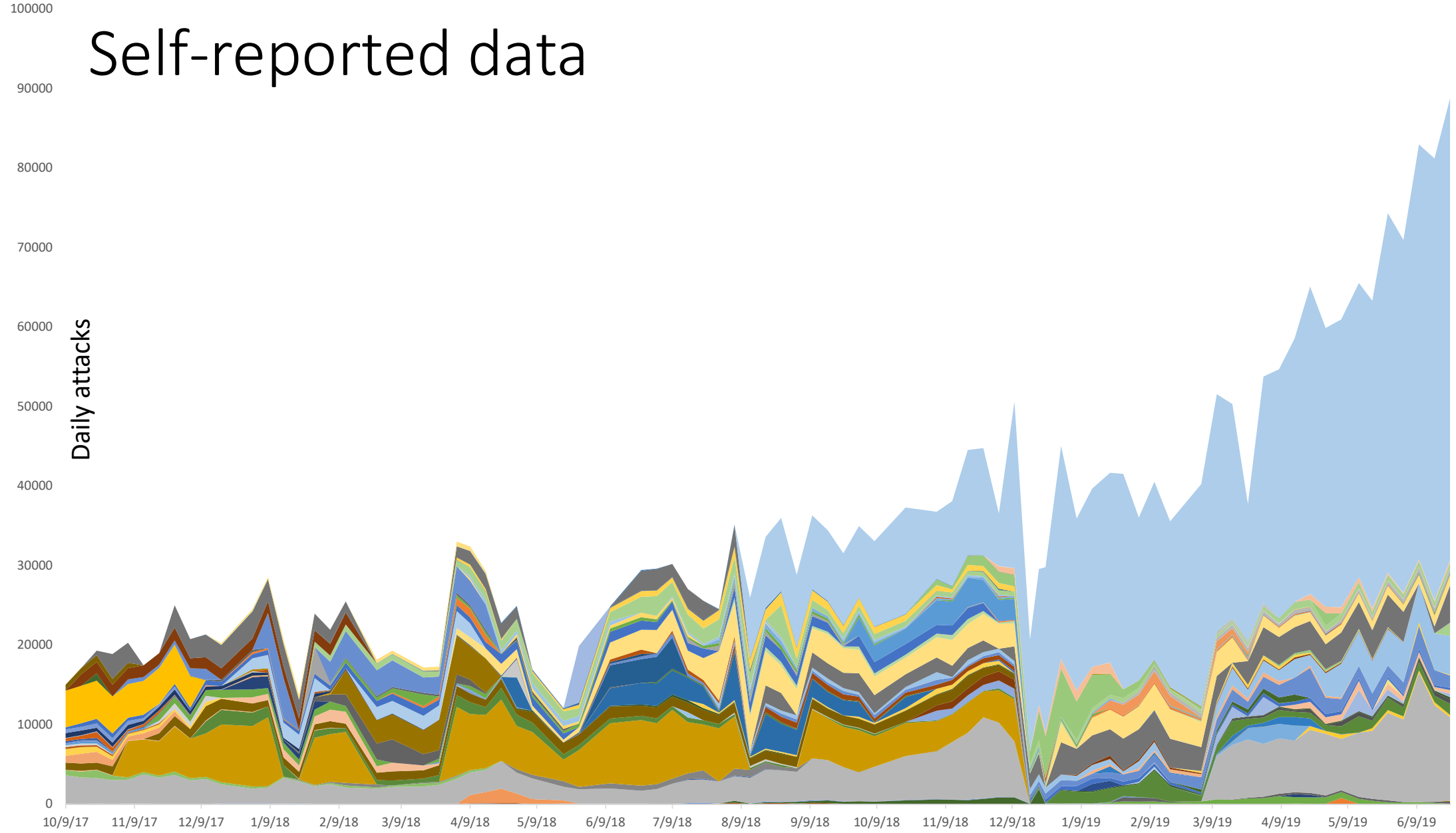
- Sentencing – indeterminate, smallish 2 week dips, localized
- Takedown (widespread) – deep cut to the market, growth suppressed for around 10 weeks
- Arrest – single arrest shows only two week effect
- Messaging – very interesting

Intervention		UK	US	RU	FR	DE	PL	NL	Overall
Xmas2018 Intervention 19/12/2018	Mean	-41%	-49%	-19%	-11%	-32%	-49%	-25%	**-39%**
	L95/U95	-49/-32%	-56/-41%	-39/9%	-22/2%	-40/-23%	-62/-31%	-39/-8%	-43/-33%
	Duration	9 weeks	11 weeks	N/A	N/A	8 weeks	2 weeks	8 weeks	10 weeks
	Signif.	0.000**	0.000**	0.163	0.091	0.000**	0.000**	0.006*	0.000**
Mirai #1 18/09/2018	Mean	-26%	-28%	9%	14%	-17%	-34%	-20%	**-12%**
	L95/U95	-36/-15%	-40/-14%	-16/41%	-6/39%	-29/-4%	-48/-17%	-33/-5%	-18/-6%
	Duration	1 weeks	2 weeks	N/A	N/A	5 weeks	6 weeks	7 weeks	8 weeks
	Signif.	0.000**	0.000**	0.5	0.1	0.013*	0.000**	0.01*	0.000**
Mirai #2 26/10/2018	Mean	21%	-32%	-23%	-20%	-16%	-21%	-32%	**-35%**
	L95/U95	-29/104%	-46/-16%	-45/9%	-39/5%	-35/7%	-35/-5%	-41/-20%	-42/-27%
	Duration	N/A	3 weeks	N/A	N/A	N/A	4 weeks	2 weeks	3 weeks
	Signif.	0.482	0.000**	0.136	0.107	0.164	0.015*	0.000**	0.000**
Webstresser 24/04/2018	Mean	-17%	-20%	23%	-31%	-37%	-36%	144%	**-25%**
	L95/U95	-29/-3%	-30/-7%	-11/71%	-44/-16%	-46/-26%	-49/-19%	85/222%	-34/-16%
	Duration	2 weeks	5 weeks	N/A	4 weeks	4 weeks	6 weeks	4 weeks	3 weeks
	Signif.	0.02*	0.002*	0.212	0.000**	0.000**	0.000**	0.000	0.000**
Titaniumstresser sentencing 25/04/2017	Mean	-47%	-34%	-38%	-36%	-37%	-38%	-32%	**-37%**
	L95/U95	-55/-39%	-41/-26%	-58/-9%	-56/-6%	-51/-20%	-66/15%	-51/-8%	-43/-31%
	Duration	2 weeks	2 weeks	2 weeks	2 weeks	2 weeks	2 weeks	2 weeks	2 weeks
	Signif.	0.000**	0.000**	0.016*	0.024*	0.000**	0.13	0.014*	0.000
HackForums 28/10/2016	Mean	-45%	-38%	-16%	-53%	-36%	0%	-38%	**-28%**
	L95/U95	-51/-39%	-48/-26%	-29/-1%	-59/-46%	-45/-27%	-20/24%	-47/-28%	-36/-20%
	Duration	15 weeks	8 weeks	8 weeks	15 weeks	7 weeks	N/A	15 weeks	9 weeks
	Signif.	0.000**	0.000**	0.042*	0.000**	0.000**	0.965	0.000**	0.000**
Unknown disruption 23/02/2018	Mean	13%	-8%	6%	-19%	-18%	37%	-19%	**-12%**
	L95/U95	-27/2%	-20/5%	-13/28%	-31/-5%	-28/-7%	15/63%	-32/-4%	-18/-7%
	Duration	N/A	N/A	N/A	2 weeks	2 weeks	2 weeks	2 weeks	2 weeks
	Signif.	0.085	0.232	0.5	0.009*	0.002*	0.000**	0.017*	0.000**

NCA intervention



Self-reported data



Quantitative findings - summary

- Largely able to link interventions to drops in the attack time series (accounting for trend and seasonality)
- Countries appear to have de-linked over time
- Messaging - surprisingly large effect from the NCA intervention
- Sentencing appears to have no consistent effect, but doesn’t stimulate the market in the way it does for cryptomarkets. Effects are limited to a couple of weeks where they do occur
- Single takedowns and arrests do little
- Wide-scale takedowns significantly impact the market (Hackforums and FBI Christmas Operation)
- Surprisingly brittle to intervention

Qualitative analysis

- Interviews with booter providers
- Scraping public forums and chat channels

Chat channels and message groups

- Scraped hundreds of channels
- Discord a site where a lot of cybercrime is happening
- Channels very unstable
- Publicly advertised
- Business and community
- Links to other kinds of crime – credit card fraud, illegal software, hacks etc.
- But – communities tend to be fairly small
- Many have moved to Telegram since the arrests
- Largely used by smaller providers to drum up business and maintain trust

Brittle community – key factors

- Community
- Provider
- User

Community factors

- Hackforums – dispersion of community
- Weak cultural capital

Provider factors

- Very dependent on small number of server providers – the people who run the infrastructure
- Several left in the wake of the FBI raid, which had a huge impact on many booters
- Some old ones who had “got out of the game” set their booters back up for a fortnight immediately after the raid
- This job is extremely boring and relatively low-paid – effectively a low-level admin job
- Relatively low levels of technical skill – source methods from Pastebin, or buy from private sellers

“Its so unpredictable. I expect the community surrounding it to die. There will always be a demand for ddos. Lots of factors. Lots of people are starting to see what I and lots of others see. A place where you learn nothing new and do not go much of anywhere. [I think people will] disengage entirely [rather than move onto other types of crime] That’s what I pretty much did”

Booter provider

“And after doing for almost a year, I lost all motivation, and really didn’t care anymore. So I just left and went on with life. It wasn’t challenging enough at all. Creating a stresser is easy. Providing the power to run it is the tricky part. And when you have to put all your effort, all your attention. When you have to sit infront of a computer screen and scan, filter, then filter again over 30 amps per 4 hours it gets annoying”

Booter provider

User factors

- High user turnover, users are young, and dependent on some fairly flimsy neutralisations
- Pervasive idea that DDoS is legal, low-harm
- Mutual shifting of risk – providers claim that their terms of service protect them, users believe (correctly) that providers are taking the bigger risk
- No strong value system or culture
- Apart from the bigger providers somewhat of a lemon market – lifetime plans etc. are risky purchase as most fold after a few weeks
- Fold due to a number of factors – natural exit, but also unique problems with growing too fast
- Basically zero technical skill – so any security hardening makes services inaccessible

Concluding thoughts

- Booting particularly susceptible to interventions
- Messaging and wide-ranging takedowns appear to suppress the market
- Little to no effect from harsh sentencing
- Arrests have little effect on the broader market
- Easier to stop new people getting involved than to dissuade existing users – but high turnover so may be a long-term strategy – normative rather than deterrent