Booting the booters

Ben Collier, Daniel R. Thomas, Richard Clayton, Alice Hutchings

Firstname.Lastname@cl.cam.ac.uk
The booter market is vulnerable

- Interventions work (unusual)
  - Widespread arrests and takedowns
  - Closure of Hackforums booter section
  - Advertising

- Target server managers
  - Have mid-level technical (administrative) skills
  - Work is tedious and low-status
big.gov IN TXT "Extremely long response.................

.............................."

src: 8.8.8.8
dst: 172.16.6.2

172.16.6.2

Attacker
192.168.25.4
Boo‡er services scale DDoS users

● 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
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
<table>
<thead>
<tr>
<th>Pricing Plan</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>BASIC-1</td>
<td>$9.99 USD</td>
</tr>
<tr>
<td>BASIC-2</td>
<td>$19.99 USD</td>
</tr>
<tr>
<td>BASIC-3</td>
<td>$25.99 USD</td>
</tr>
<tr>
<td>BASIC-4</td>
<td>$29.99 USD</td>
</tr>
<tr>
<td>BASIC-5</td>
<td>$34.99 USD</td>
</tr>
<tr>
<td>BASIC-6</td>
<td>$44.99 USD</td>
</tr>
</tbody>
</table>

**Features:**
- **Attacks per day:** unlimited
- **Attack time:** 5 min
- **Attack power:** 15 Gbit/s
- **Concurrent attacks:** 1
- **Layer 4 methods:** ✓

**Subscription:**
- [Sign Up & Buy now](#)
**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.
Booters: Dispersed but advertised

- 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, many resell capacity from the top ten
Collection 1: UDP-reflection attacks from honeypots

- Median 65 nodes since 2014
- Hopscotch emulates abused protocols: QOTD, CHARGEN, DNS, NTP, SSDP, SQLMon, Portmap, mDNS, LDAP
- Sniffer records all resulting UDP traffic
- (try to) Only reply to black hat scanners
- Attack: Flow to an IP(prefix) where more than 5 packets received by one sensor

Ethics: Absorb attack traffic, don’t reply to white hat scanners

Collection 2: Booter self-reports (are reliable)

- Collected from booter websites which report running total
- Covers 75% of active booters over 18 month period
- Source code and leaked databases show generally accurate (bad data excluded)
- Heteroskedasticity and skewness kurtosis tests indicate not faked
- Correlate with Collection 1 and with interventions.
PRESENTER
SWITCH
Intervening is hard

- Intervening in offline illegal markets is challenging
- Intervening in online illegal markets is EVEN MORE challenging
- These tend to be highly resilient (e.g. cryptomarkets)
- High levels of displacement
- Still little understanding of best practice
We considered four types of intervention

- Arrests
- Sentencing
- Messaging
- Takedowns - example
This website has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Central District of California under the authority of 18 U.S.C. §1030(j)(1)(A) as part of coordinated law enforcement action taken against illegal DDoS-for-hire services.

This action has been taken in coordination with the United States Attorney’s Office of the District of Alaska, the Department of Justice Computer Crime and Intellectual Property Section, and

For additional information, see the FBI Public Service Announcement L-101717b-PSA, https://www.ic3.gov/media/2017/171017-2.aspx
Example takedown - FBI operation

- 20th December 2018
- Distributed Denial of Service as a Services (booters / stressers) targeted
- 3 arrests
- 15 domains seized, 7 booters
Modelling

- Negative binomial regression
- Time series of weekly totals and by country
- ‘Intervention’ variables for all big drops, keep significant ones
Largely able to link interventions to drops in the attack time series (accounting for trend and seasonality)

- Observed attacks
- Model
- Interventions

Key events:
- Hackforums closes booter section
- VDOS sentencing
- Webstresser takedown
- Mirai sentencing
- Xmas 2018 event
Booters: Surprisingly brittle to 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 and only where other stuff going on
- Single takedowns and arrests do little
- Wide-scale takedowns significantly impact the market (Hackforums and FBI Christmas Operation)
- Messaging - surprising effect!
Messaging: Surprisingly large effect from the NCA intervention
Results 2: self-reported (my favourite slide)

Webstresser arrest

FBI takedowns
Analysis

- Less resilient than other kinds of cybercrime (we think)
- Single arrests and sentencing do little
- But hitting the infrastructure and messaging campaigns work
Why: Qualitative results

- Interviews and scraping chat channels
- Booting is rubbish! Low cultural capital
- High user turnover - so if you can stop people getting involved, big effect
- Lots of centralisation reselling makes the market brittle to infrastructural intervention
- Depends on a relatively small number of server managers
- Who have a boring and unrewarding job, so easy to dissuade
- Especially when you make their job even more annoying by messing with the infrastructure!
USE OUR DATA

Talk to us about future work

ben.collier@cl.cam.ac.uk

@johnnyhistone

d.thomas@strath.ac.uk

@DanielRThomas24

https://www.cambridgecybercrime.uk/process.html