DDoS Hide & Seek: On the Effectiveness of a Booter Services Takedown

Oliver Hohlfeld
Overloading the Web Server

Distributed Denial of Service Attack
Performing DDoS Attacks

Requires

- technical expertise
- infrastructure
  - Use somebody else’s infrastructure
  - protocol flaws, unprotected systems, ...
I am lacking expertise: let me Google it

The perils of **boother services**

Fact is that, as long as they are allowed to operate with relative impunity, these **DDoS-for-hire services** can endanger entire online industries, especially SaaS and e-commerce that are built on user-trust and constant availability.
[Demo]
What is known about Booters

- Analysis of booter leaked customer databases [NM’15], [USENIX LEET’13]

- Victims: [Springer Attacks, Intrusions & Defenses’16]

- Booter blacklists & website fingerprinting [NM’18], [CNSM’16], [Collab. Comput. Conf.’18]

- Blacklist based booter market study [Commag’17]
Do they deliver what they promised?
Let’s try to **attack our own infrastructure**
Measurement Infrastructure

IXP

Our measurement AS

...
Buying Booter Services

| Booter | Seized  | Time     | NTP | DNS | CLDAP | mcache | non-VIP | VIP     |
|--------|---------|----------|-----|-----|-------|--------|---------|---------|
| A      | ✓       | Apr, Aug | ✓   | ✓   | ✓     | ✓      | $8.00   | $250    |
| B      | ✓       | Jun-Sep  | ✓   | ✓   | ✓     | ✓      | $19.83  | $178.84 |
| C      |         | Apr-May  | ✓   | ✓   |       |        | $14.00  | $89     |
| D      |         | May      | ✓   | ✓   |       |        | $19.99  | $149.99 |

- Booter B offers:
  - Cheaper non-VIP services: 8-12 Gbps
  - More expensive VIP services: 80-100 Gbps
Cheaper, non VIP Services

The diagram shows the traffic in Mbps against the number of reflectors and peers for different booter services. The booter services are categorized as:

- booter A NTP
- booter A NTP (no transit)
- booter B CLDAP
- booter B memcached
- booter B NTP 1
- booter B NTP 2
- booter B NTP (no transit)
- booter C NTP
- booter C NTP (no transit)
- booter C NTP
- booter D NTP

The data is sorted by date, with a high overlap between different booters. The traffic varies significantly, with peaks of about 7000 Mbps for some booters. The number of reflectors and peers also varies, with some booters having a large number of reflectors but fewer peers, while others have a smaller number of reflectors but more peers.

The diagram indicates that booter A NTP and booter A NTP (no transit) have the highest traffic, with booter D NTP having the lowest traffic. The number of reflectors and peers also varies significantly, with some booters having a large number of reflectors but fewer peers, while others have a smaller number of reflectors but more peers.

The data suggests that booter A NTP and booter A NTP (no transit) are the most effective booter services, while booter D NTP is the least effective. The number of reflectors and peers also varies significantly, with some booters having a large number of reflectors but fewer peers, while others have a smaller number of reflectors but more peers.
More expensive, VIP services

Almost immediate start

controlled stop

Gbps

duration (sec)

NTP VIP DDoS
Memcached VIP DDoS

0.0
1.0
2.0
3.0
4.0
5.0
6.0
7.0
8.0
9.0
10.0
11.0
12.0
13.0
14.0
15.0
16.0
17.0
18.0
19.0
20.0

0
50
100
150
200
250
300
350
It works
We’re not the only ones knowing that
December 2018

15 booter domains
This domain 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(i)(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 I-101717b-PSA, https://www.ic3.gov/media/2017/171017-2.aspx
FBI kicks some of the worst ‘DDoS for hire’ sites off the internet

Zack Whittaker
@zackwhittaker / 8:38 pm CET • December 20, 2018

The FBI has seized the domains of 15 high-profile distributed denial-of-service (DDoS) websites after a coordinated effort by law enforcement and several tech companies.
Domain Perspective on FBI Takedown

- Data: weekly snapshots of all 140M .com/.net/.org domain
  - DNS
  - HTTPS
  - August 2016 – April 2019

- Keyword search: “booter”, “stresser”, “ddos-as-a-service”, … (following booterblacklist.com)

- Many alternative (non-seized) booter sites exist
more popular booter sites exist

before take down

after take down

seized domains remain popular

even gain in popularity

Seized booter papers popular, but not the most popular ones
Did this takedowns had any effect?
Vantage Points

IXP  
- October 27 – January 31
- 834 B flows

Tier-1  
- December 12 – December 31
- 6.6 B flows

Tier-2  
- September 27 – February 2
- 470 M flows
NTP DDoS Attacks in the Wild

- 311K destinations (Tier-1 ISP: 36K, Tier-2 ISP: 95K, IXP: 244K) that receive NTP reflection traffic
- Conservative filtering / view: 69k destinations
- 224 victims receives > 100 Gbps,
  5 > 300 Gbps
  1 > 600 Gbps
IXP: Systems under NTP DDoS attack per hour

![Graph showing NTP DDoS attacks per hour over time. The graph includes dates from 18/09/30 to 19/01/28. The y-axis represents the count of NTP attacks, and the x-axis represents the date of measurement. SHAP signs indicate periods of high activity, with shaded areas highlighting significant events.]

- wt30 sign. (p=0.05): False
- wt40 sign. (p=0.05): False

Large IXP perspective

+40 day window
+30 day window
takedown operation

count of NTP attacks

date of measurement

The graph shows the count of NTP DDoS attacks per hour over a period from 18/09/30 to 19/01/28. SHAP signs indicate periods of high activity, with shaded areas highlighting significant events. The y-axis represents the count of NTP attacks, and the x-axis represents the date of measurement. The graph includes dates from 18/09/30 to 19/01/28. The y-axis represents the count of NTP attacks, and the x-axis represents the date of measurement.
Domain Perspective on FBI Takedown

- Data: weekly snapshots of all 140M .com/.net/.org domain
  - DNS
  - HTTPS

- Keyword search: “booter”, “stresser”, “ddos-as-a-service”, … (following booterblacklist.com)

- Many alternative (non-seized) booter sites exist

- Booter A became active with a new domain 2 days after seizure
  - Domain registered in mid 2018
  - Even our login credentials still work ;)

Chair of Computer Networks
Conclusions

- Booters: user friendly and cheap way to launch DDoS attacks
  - You mostly get what you pay for

- There is lots of DDoS attack traffic in the Internet

- Law enforcement action in December 2018 had little success
  - One booter became active quickly after take down
  - Short-time reduction of requests to amplifiers
  - No effect of take down on attack traffic reflected by amplifiers