DDoS Hide and Seek –
On the Effectiveness of a Booter Service Takedown

D. Kopp¹, M. Wichtlhuber¹, I. Poese², J. Santanna³, O. Hohlfeld⁴, C. Dietzel¹,⁵

DE-CIX¹, BENOCS², University of Twente³, BTU⁴, MPI⁵
DDoS Attacks and Booter

Requirements

• Technical expertise (about tools, network and coding)
• Infrastructure (use other infrastructure, protocol flaws, unprotected systems, ...)

? Gbps
DDoS Attacks and Booter

→ Requirements

- Technical expertise (about tools, network and coding)
- Infrastructure (use other infrastructure, protocol flaws, unprotected systems, ...)

10 Gbps
Booster Services

→ DDoS-as-a-service
  • Web interface
  • Easy to find and use

→ One klick to start a DDoS
  • To any IP or domain

→ Pretend to be legal
Attacks and Service Levels

→ 10 - 20 different protocols (UDP, DNS..)
  • Application → high pps
  • Amplification → high bandwidth

→ Service plans differ by
  • Number concurrent attacks
  • Length of attacks

→ Claim to offer
  • 5 - 12 Gbps basic from 10$
  • 80 - 100 Gbps VIP more than 80$
Attacks and Service Levels

→ 10 - 20 different protocols (UDP, DNS..)
  • Application → high pps
  • Amplification → high bandwidth

→ Service plans differ by
  • Number concurrent attacks
  • Length of attacks

→ Claim to offer
  • 5 - 12 Gbps basic from 10$
  • 80 - 100 Gbps VIP more than 80$
FBI kicks some of the worst ‘DDoS for hire’ sites off the internet

Zack Whittaker

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

THIS WEBSITE HAS BEEN SEIZED

For additional information, see the FBI Public Service Announcement 1-101717b-PSA, https://www.ic3.gov/media/2017/171017-2.aspx
Research Questions and Contribution

→ What’s the threat of booter attacks?
  • Unique active measurement setup
  • Anatomy and state of booter DDoS attacks
  • Measurement of VIP DDoS

→ What’s the status quo of DDoS attacks?
  • NTP DDoS attacks at IXP, Tier-1 and Tier-2 ISP

→ What’s the effect on attacks and traffic after the take down of 15 booters?
**Measurement System**

→ **Internet Connectivity**
   - 10 Gigabit link IXP peering
   - 10 Gigabit transit
   - Own AS and IPv4 space

→ **Measurement Limitations**
   - up to 10 Gbps → packet capture
   - over 10 Gbps → flow data
## Selection of Booter Services

<table>
<thead>
<tr>
<th>Booter</th>
<th>Seized</th>
<th>Time</th>
<th>NTP</th>
<th>DNS</th>
<th>CLDAP</th>
<th>mcache</th>
<th>non-VIP</th>
<th>VIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>✓</td>
<td>Apr, Aug</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>$8.00</td>
<td>$250</td>
</tr>
<tr>
<td>B</td>
<td>✓</td>
<td>Jun-Sep</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>$19.83</td>
<td>$178.84</td>
</tr>
<tr>
<td>C</td>
<td></td>
<td>Apr-May</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>$14.00</td>
<td>$89</td>
</tr>
<tr>
<td>D</td>
<td></td>
<td>May</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>$19.99</td>
<td>$149.99</td>
</tr>
</tbody>
</table>

- **four booter services tested**
- **attack types recorded**

**Tested VIP service**
Non-VIP Booter DDoS Attacks

→ 100 – 1000 reflectors
→ max. 7 Gbits
→ NTP attacks 80% via transit
→ Memcached 80% via IXP

→ NTP attacks are the most significant attacks
**VIP Booter DDoS**

- **NTP DDoS up to 20 Gbit/s**
  - 930 source IPs (reflectors)
  - 350 source ASNs (networks)

- **Memcached DDoS up to 13 Gbit/s**
  - NTP most significant attack

**Graph**
- Immediate start
- Controlled stop
- Transit connection died
Distribution of NTP Packet Sizes

- Small → NTP queries
- Large → Monlist replies
- Split at 50% for small and large packets

We use 200 bytes as a filter to find DDoS attacks
Passive Measurement Vantage Points

- **IXP**
  - October 27 – January 31 (3.5 months)
  - 834 Billion flows

- **Tier-1**
  - December 12 – December 31 (3 weeks)
  - 6.6 Billion flows

- **Tier-2**
  - September 27 – February 2 (4.5 months)
  - 470 Million flows
NTP DDoS Attacks in the Wild

→ We profile attack traffic
  • Number of reflectors
  • Max GBytes per second

→ 311K destinations

224 victims > 100 Gbps
5 > 300 Gbps
1 > 600 Gbps
**NTP DDoS Attacks in the Wild**

→ We profile attack traffic
  - Number of reflectors
  - Max GBytes per second

→ 311K destinations

224 victims > 100 Gbps
5 > 300 Gbps
1 > 600 Gbps
NTP DDoS Attacks in the Wild

→ We profile attack traffic
  • Number of reflectors
  • Max GBytes per second

→ 311K destinations

224 victims > 100 Gbps
5 > 300 Gbps
1 > 600 Gbps
**NTP DDoS Attacks in the Wild**

→ We profile attack traffic
  - Number of reflectors
  - Max GBytes per second

→ 311K destinations

224 victims > 100 Gbps
5 > 300 Gbps
1 > 600 Gbps
NTP DDoS Attacks in the Wild – Anomalies

➔ Two filter criteria for anomalies:
   1. Traffic > 1 Gbps
   2. More than 10 sources

➔ Conservative filtering:
   69k destinations
NTP DDoS Attacks in the Wild – Anomalies

- Two filter criteria for anomalies:
  1. Traffic > 1 Gbps
  2. More than 10 sources

- Conservative filtering: 69k destinations
NTP DDoS Attacks in the Wild – Anomalies

- Two filter criteria for anomalies:
  1. Traffic > 1 Gbps
  2. More than 10 sources

- Conservative filtering:
  69k destinations

We use this filtering criteria to investigate attacks over time
Booter Services vs. FBI

→ FBI operation took down prox. 15 DDoS for hire services Dec. 20, 2018
We are the first to report the capabilities of a premium (VIP) booter service that peaks at 20 Gbps while promising 60-80 Gbps. In our consideration of a major IXP, a tier-1 ISP, and a tier-2 ISP—with a focus on the ecosystem of booters, as well as our colleague Tim Träris, and our significant gains to possible victims, as the underlying infrastructure of re-confirmation, or involved entities.

We thank the IMC anonymous reviewers and our shepherd, J. Alex Halderman (University of Michigan), for their constructive comments, as well as our colleague Tim Träris, and our significant gains to possible victims. To exclude false positives, we use more reliable vectors to victims.

Nevertheless, we could not extract any signifiers from Sections 4 and 30/40 days after the takedown.

Figure 4: Selected signifiers for NTP DDoS learned from our self-attacks, which shows no significant reduction in attack traffic when comparing 30/40 days before and after the takedown; Figure 5: Systems under NTP DDoS attack per hour.
This paper studies for the first time the e-commerce, e.g., on infrastructures, need to better study the ecosystem of booter service domains in total increased over the measurement period despite the seizure. Our study aims to inform network operators to better understand the current threat-level, but also law enforcement agencies to assess the health of the booter ecosystem. This motivates the technical parameters, the question arises whether this is sufficient to shut down or block open re-runners to better understand the current threat-level, but also law enforcement agencies to assess the health of the booter ecosystem. This motivates the technical parameters, the question arises whether this is sufficient to shut down or block open re-runners.

We are the first to report the capabilities of a premium (VIP) booter service that peaks at 20 Gbps while promising 60-80 Gbps. In our consideration of popular booters, we study booter capabilities. The technical parameters, the question arises whether this is sufficient to shut down or block open re-runners to better understand the current threat-level, but also law enforcement agencies to assess the health of the booter ecosystem. This motivates the technical parameters, the question arises whether this is sufficient to shut down or block open re-runners to better understand the current threat-level, but also law enforcement agencies to assess the health of the booter ecosystem.

To study if booter takedowns of law enforcement agencies help to possibly reduce the attack traffic, we analyze the effect on the DDoS amplification traffic from multiple perspectives. We consider the infrastructure of re-runners, as the underlying infrastructure of re-booter services does not improve the situation for DDoS vectors to victims. To exclude false positives, we use more reliable indicators for NTP DDoS learned from our self-attacks, which shows no correlation with the number of systems attacked.

Nevertheless, we could not find any correlation with the number of systems attacked. To study if booter takedowns of law enforcement agencies help to possibly reduce the attack traffic, we analyze the effect on the DDoS amplification traffic from multiple perspectives. We consider the infrastructure of re-runners, as the underlying infrastructure of re-booter services does not improve the situation for DDoS vectors to victims. To exclude false positives, we use more reliable indicators for NTP DDoS learned from our self-attacks, which shows no correlation with the number of systems attacked.

Nevertheless, we could not find any correlation with the number of systems attacked. To study if booter takedowns of law enforcement agencies help to possibly reduce the attack traffic, we analyze the effect on the DDoS amplification traffic from multiple perspectives. We consider the infrastructure of re-runners, as the underlying infrastructure of re-booter services does not improve the situation for DDoS vectors to victims. To exclude false positives, we use more reliable indicators for NTP DDoS learned from our self-attacks, which shows no correlation with the number of systems attacked.

Nevertheless, we could not find any correlation with the number of systems attacked. To study if booter takedowns of law enforcement agencies help to possibly reduce the attack traffic, we analyze the effect on the DDoS amplification traffic from multiple perspectives. We consider the infrastructure of re-runners, as the underlying infrastructure of re-booter services does not improve the situation for DDoS vectors to victims. To exclude false positives, we use more reliable indicators for NTP DDoS learned from our self-attacks, which shows no correlation with the number of systems attacked.

Nevertheless, we could not find any correlation with the number of systems attacked. To study if booter takedowns of law enforcement agencies help to possibly reduce the attack traffic, we analyze the effect on the DDoS amplification traffic from multiple perspectives. We consider the infrastructure of re-runners, as the underlying infrastructure of re-booter services does not improve the situation for DDoS vectors to victims. To exclude false positives, we use more reliable indicators for NTP DDoS learned from our self-attacks, which shows no correlation with the number of systems attacked.

Nevertheless, we could not find any correlation with the number of systems attacked. To study if booter takedowns of law enforcement agencies help to possibly reduce the attack traffic, we analyze the effect on the DDoS amplification traffic from multiple perspectives. We consider the infrastructure of re-runners, as the underlying infrastructure of re-booter services does not improve the situation for DDoS vectors to victims. To exclude false positives, we use more reliable indicators for NTP DDoS learned from our self-attacks, which shows no correlation with the number of systems attacked.

Nevertheless, we could not find any correlation with the number of systems attacked. To study if booter takedowns of law enforcement agencies help to possibly reduce the attack traffic, we analyze the effect on the DDoS amplification traffic from multiple perspectives. We consider the infrastructure of re-runners, as the underlying infrastructure of re-booter services does not improve the situation for DDoS vectors to victims. To exclude false positives, we use more reliable indicators for NTP DDoS learned from our self-attacks, which shows no correlation with the number of systems attacked.

Nevertheless, we could not find any correlation with the number of systems attacked. To study if booter takedowns of law enforcement agencies help to possibly reduce the attack traffic, we analyze the effect on the DDoS amplification traffic from multiple perspectives. We consider the infrastructure of re-runners, as the underlying infrastructure of re-booter services does not improve the situation for DDoS vectors to victims. To exclude false positives, we use more reliable indicators for NTP DDoS learned from our self-attacks, which shows no correlation with the number of systems attacked.

Nevertheless, we could not find any correlation with the number of systems attacked. To study if booter takedowns of law enforcement agencies help to possibly reduce the attack traffic, we analyze the effect on the DDoS amplification traffic from multiple perspectives. We consider the infrastructure of re-runners, as the underlying infrastructure of re-booter services does not improve the situation for DDoS vectors to victims. To exclude false positives, we use more reliable indicators for NTP DDoS learned from our self-attacks, which shows no correlation with the number of systems attacked.
Changes in DDoS Traffic

→ Statistically significant changes 30/40 days around takedown

→ We investigate NTP, DNS, Memcached

• IXP Memcached destination
• Tier-2 ISP NTP destination

→ We find: Only traffic towards reflectors was affected

→ No significant changes in direct attack traffic
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) [J. Santanna et. al.]
→ Search for available, new booter webpages and twins
more popular booter sites exist

before take down

after take down

seized domains remain popular
even gain in popularity
Domain Perspective on FBI Takedown

→ Many **alternative** (non-seized) **booster sites exist** (58 for .com/.net/.org)

→ **Seized booster** papers popular, but **not the most popular** ones

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


Conclusion

→ Booters: user **friendly, cheap and popular** way to launch DDoS attacks
  - You mostly get what you pay for but a lower bandwidth
  - NTP DDoS attacks are the most potent
  - Attacks size critical to most small to medium networks

→ There is lots and permanent DDoS attack traffic in the Internet

→ Law enforcement action in December 2018
  - One booter became **active quickly after take down**
  - Short-time reduction of request traffic to amplifiers
  - Little effect on traffic reflected by amplifiers and attack count