Lecture 24 – Networking Attacks in Practice: DDoS Ecosystem

Ryan Cunningham
University of Illinois
ECE 422/CS 461 – Fall 2017
Security News

• Kaspersky claims NSA tools picked up by legit malware scan
• Krebs write up on Reaper botnet: spreading as a slow scanning worm
• “Bad Rabbit” ransomware spreading in Ukraine and Russia
Understanding the Emerging Threat of DDoS-as-a-Service

Mohammad Karami and Damon McCoy
George Mason University
What this Talk is About

• Booter services are commoditizing DDoS

• DDoS as subscription based service
  – Tiered pricing (Payment via PayPal)
  – Easy to use website interface
  – Ability to DDoS medium-end webservers

• Use leaked backend data from TWBooster to gain insight
Quantum Booter - Stress Testing Service
quantumbooter.net/
Quantum Booter utilizes high powered dedicated servers to stress test. We are constantly upgrading our servers to fulfill the power needs of our clients. We only ...

Grim Booter
grimboot.com/tos.php
Permission is granted to stress test dedicated servers and networks owned by you. ... You are liable for what you do at http://grimboot.com, if you break any of ...

DESTRESS BOOTER Home
destressbooter.com/
THE BEST BOOTER. ... Protected. Destress Booter is powered by quick, strong, and DDoS protected servers to guarantee uptime and stability. With the ...

Orion Booter - Powered by InfernoAPI
www.orionbooter.com/
We are not responsible how you use this booter, the website was meant to be used as a stress network tester. 4. Sharing your account will result in suspension ...

ToxicBoot | Login
toxicboot.net/
Login. Username: Password: By Logging in you agree to all Terms of service.

Opaque Booter - Home
opaquebooter.weebly.com/
Create a free website with Weebly. Quantum Booter. Affordable and professional stress testing service. Main · Stress Test · User CP · Forums · Tools · Logout ...

[FREE] JabXBooter | Stress Tester | UDP | 250+ Shells *Powerful ...
www.hackcommunity.com › ... › Hacking Tools and Similar Applications.
Sep 28, 2011 - 10 posts - 4 authors
RE: [FREE] JabXBooter | Stress Tester | UDP | 250+ Shells *Powerful. Booters are worthless, but that’s my opinion. RAT servers 4ever lol ...
DDOS EM’
When In Doubt Knock Em’ Out!

Features

Resolvers
- Skype
- Steam
- Cloudflare

IP Tools
- Geolocation
- IP Logger
- Host to IP

Max Boot Time Of
3600
UDP, SSYN, RUDY, UDP-LAG, ARME, GET, POST
How to Setup Booter Service

• Step 1: Website code
  – Asylumbooter source code is available at: http://softwaretopic.informer.com/asylum-booter-source/

• Step 2: Attack Infrastructure
  – Rent or use compromised servers

• Step 3: Establish payment via PayPal

• Step 4: Advertise on Hackforums and Gamer sites

• Step 5: Profit $$$
### Dataset

- Publicly post backend data from TWBooter2

<table>
<thead>
<tr>
<th>Duration</th>
<th>Users</th>
<th>Victims</th>
<th>Attacks</th>
</tr>
</thead>
</table>

- Includes information on all attacks
  - IP/Domain targeted, type, duration, client
  - Confirmed details of attacks with one victim

- Provides insight into infrastructure, users, and victims
Used to Target Bloggers
Attack Infrastructure

• 15 servers total servers
  – 3 active the entire two months
  – Most hosted at a Netherlands ISP
  – 9 active at the time of data leak

• Offered SYN flood, UDP flood and amplification attacks, HTTP-based attacks including HTTP POST/GET/HEAD and RUDY (R-U-Dead-Yet)
Attack Capacity

• Subscribed to service to measure capacity.

• SYN Floods spoof IP

• UDP Flood uses DNS amplification

<table>
<thead>
<tr>
<th>Attack Type</th>
<th># of packets</th>
<th>Avg. packet size</th>
<th>Volume</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP Flood</td>
<td>4,552,899</td>
<td>1,363 bytes</td>
<td><strong>827 MBit/sec</strong></td>
</tr>
<tr>
<td>SYN Flood</td>
<td>5,625,086</td>
<td>54 bytes</td>
<td><strong>40 MBit/sec</strong></td>
</tr>
</tbody>
</table>

• HTTP used 26,296 proxy servers over 5 mins
  – Some of these leaked original attack servers IPs
User Growth Rate

- After initial burst growth rate of 3.2 Users
User Subscriptions

• Categorized users based on subscription type
  – Gamers <= 10 Min attacks (65%)
  – Website >= 1 hour attacks (32%)
  – Privileged unlimited attacks (3%)

• TwBooter earned $7,727/month based on subscription type
User Attacks

• 6 users are responsible for half (28,154 hours) of the attack time.

<table>
<thead>
<tr>
<th></th>
<th>Gamers</th>
<th>Website</th>
<th>Privileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of users</td>
<td>180</td>
<td>41</td>
<td>8</td>
</tr>
<tr>
<td>Avg distinct targets per day</td>
<td>3.32</td>
<td>3.46</td>
<td>2.86</td>
</tr>
<tr>
<td>Avg attacks per day</td>
<td>13</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>Avg attack time per day</td>
<td>59 m</td>
<td>14 h</td>
<td>105 h</td>
</tr>
</tbody>
</table>
Victims

• 10,485 unique IP addresses attacked

• 689 identified as websites
  – Most are either game servers or game forums
  – Other booters and bloggers also targeted

• Two users attacked government sites for 142 hours
  – Two Indian government
  – Los Angeles police department
Other Booter Services

• Leaks backend for Asylumbootsr
  – Shows 5,622 subscribers
  – almost half a million attacks over 16 months

• More backends can be found on pastebin
  – Show evidence of compromised servers used as attack infrastructure
  – Hacked into by “vigilante” groups, such as

  [Image: BOOTER DOWN]
Conclusion

• Booters focused on low cost ($10-$200) and usability

• Integrating features such as anti-cloudflare and Skype tracking

• Uses effective DNS amplification attacks

• TWBooteer earned around $7,500/month
Understanding Booter Payment Processing

Mohammad Karami (GMU), Youngsam Park (UMD) and Damon McCoy (GMU)
Booters

• Booters have become a commoditized service

• Problem persists as long as they are profitable

• Preserved low-risk activity

• Understand payment level interventions
Bother Costs

• Direct costs
  – Attack Server Hosting + Bandwidth
  
  Private Unshared Network - 1000Mbps

  Are you a stresser owner or a heavy user? We now offer Unshared Private Networks where you have unlimited stress testing time and concurrents. Every user is assigned their own network and nobody else have access to them!

  $200 USD

  – Payment Processing 2-3% + potentially seized funds

• Indirect costs: Customer Support, IT costs, Advertising
Booter Payment Ecosystem

• Pro: Accessible for US and EU customers
• Con: Risk of account closure

• Pro: Easy to accept and limited risk of seizure
• Con: Difficult to for customers to buy into and use
Long Tail of Methods
Bitcoin Payments

• A large fraction of booters accept bitcoin

• Some accept via third party payment service
  – Converts to fiat currency and deals with hassle
  – Risk of account closure

• Some accept directly
  – Risk of tracing transactions
  – Tracing at exchange point
PayPal enforcement

• Reported 56 booter services to PayPal
  – Created auto-purchasers to track new accounts and redirection domains

• Enforcement based on referrer domain name

• PayPal investigated and limited accounts
  – Effective, but there are limitations

• Also reported to ISP hosting customer interface
  – Not effective
Aside on Website Hosting

• Cloudflare hosted all the customer facing websites for the booters we monitored
  – No response from their abuse contact

• Most domains registered with ENOM

• Only response was from GoDaddy
  – They said the associated domain, quantumbooter.net, has already been reported
  – Domain is still active 3+ months later.
# Dataset

## Overview

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experiment Period</td>
<td>2/23/2014 – now</td>
</tr>
<tr>
<td>PayPal Intervention Period</td>
<td>6/8/2014 ~ now(?)</td>
</tr>
<tr>
<td>Overall booters (including dead ones)</td>
<td>78</td>
</tr>
<tr>
<td>Reported booters</td>
<td>56</td>
</tr>
<tr>
<td>Set A (PayPal Intervention Only)</td>
<td>28</td>
</tr>
<tr>
<td>Set B (PayPal + Registrar/ISP Intervention)</td>
<td>28</td>
</tr>
</tbody>
</table>

## Classification

<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>In normal operation</td>
</tr>
<tr>
<td>Struggling</td>
<td>Booters that are unreachable or unable to receive PayPal Payment, but were in normal operation for at least one day in last two weeks</td>
</tr>
<tr>
<td>PP payment disabled</td>
<td>Booters unable to receive PayPal payments for the last two weeks</td>
</tr>
<tr>
<td>Dead</td>
<td>Booters that have been unreachable for the last two weeks.</td>
</tr>
</tbody>
</table>
**Daily Active Booters**

- **PayPal** intervention seems to be effective
- **Registrar/ISP** intervention doesn’t
Daily Booter Status

- Number of active booters is continuously decreased after PayPal intervention
Booter Reactions

• Add another payment methods
  – We're implemenenting a new autobuy system. We're going to accept BTC again.
  – Still selling subscriptions, Will be adding new methods soon. Stay tune

• Manual PayPal payment
  – Get Smacked is back! Our autobuy is not working at the moment, and we are not accepting Paypal right now. We're going to have a Bitcoin autobuy soon, and will accept Paypal possibly in the future, but it will most likely not be autobuy.

• Close the business
  – It's a shame PayPal had to shut us down several times causing us to take money out of our own pocket to purchase servers, hosting, and more.
  – We were under maintenance, sorry about that. We were only down for a couple hours.
  – Coming soon, please be patient, thank you.
Evading PayPal Detection

• Change Domain Name
  – Need to get updated domain name to customers and update ads

• Add in redirection hop to hide real domain in referrer
  – Low-cost solution to avoid limiting from paypal
  – Traceable by automated purchaser
Evading PayPal Detection

• Off-line acceptance of PayPal

----------------------------- IMPORTANT: IF YOU WANT TO PURCHASE WITH PAYPAL, PLEASE OPEN A TICKET. -----------------------------

Use the following format:

Plan you want:
PayPal E-mail:
Conclusions

• Payment interventions are effective
  – More effective on smaller ones
  – Less effective on larger ones

• Need to understand structure of booters

• Difficult problem that requires collaboration
LARGEST DDOS EVER?
Large DDoS attacks cause outages at Twitter, Spotify, and other sites

 Posted Oct 21, 2016 by Darrell Etherington (@etherington), Kate Conger (@kateconger)
Dyn DDOS

- Mirai botnet infects IoT devices with botnet
- Attacked Krebs with 620Gbps
- Attacked OVH with 1Tbps
- Attacked Dyn (1.2Tbps) and knocked Twitter, Reddit, Github, Slack, Box, Amazon, Yelp, CNN and more offline
- Attribution?