








# 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 TWBooter to gain insight

Quantum **Booter** - **Stress** Testing Service
quantum**booter**.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://**grimbooter**.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.orion**booter**.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
opaque**booter**.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 ...

| Thread / Author | Re |
| --- | --- |
| **Important Threads** | |
| **#1 Big Bang Booter [>TAKES EVERYTHING DOWN<] Skype BETA I 10800 Seconds DDoS Attacks** (Pages: 1 2 3 4 ... 57 )<br>Prime | |
| **REBOOT \| $1.99 \| 20+ GBPS \| 100% UPTIME \| LAYER 4&7 \| BETA SKYPE RESOLVER \| STOP BTN** (Pages: 1 2 3 4 ... 35 )<br>Joey | |
| **OLYMPUS STRESSER \| 12 ATTACK METHODS \| UNTRACEABLE \| CUSTOM SOURCE \| UNIQUE FEATURES** (Pages: 1 2 3 4 ... 59 )<br>MineSQL | |
| **DDoS Em \| SKYPE RESOLVER \| HOUR BOOTS WITH 25+GPBS \| EXTREMELY POWERFUL \| BEST ON HF** (Pages: 1 2 3 4 ... 13 )<br>Platinum | |
| **MASTER BOOT \| 40+GBPS \| AUTO BUY \| STOP ATTACK\| Ran by adults no BS.** (Pages: 1 2 3 4 ... 20 )<br>iNviZ | |
| **NetStress \| 12GBPS \| 3600 SECONDS \| SKYPE BETA RESOLVER \| CUSTOM SOURCE \| STOP BUTTON** (Pages: 1 2 3 )<br>Lani | |
| **xBOOT \| Drops it like it's hot \| 12 Attack Methods \| 65Gbps+ Capacity \| BEST ON HF!** (Pages: 1 2 3 4 ... 24 )<br>DaL33T | |
| **THBOOT** (Pages: 1 2 3 )<br>Dan. | |
| **Normal Threads** | |
| **Venom Stresser I 7200 Seconds Max Boot I 30GBPS I Resolvers I Takes Shit Down** (Pages: 1 2 3 )<br>Perfect | |
| **#1 Maximboot - Unlimited boot time \| 65Gbps+ \| More Features \| Stop Button \| BuyNow!** (Pages: 1 2 3 4 ... 13 ) | |




## 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

# twBooter²

Dashboard Boot Tickets Buy Account Logout

You can upgrade to paid version by completing survey, start now by clicking here

Global Message: Server replaced

Domain/Skype Resolver:

Host

Resolve

IP Address: 1.1.1.1 80

Time: 54 seconds(s)

Power: 50%

Start Attack

| IP Address | Port | Time Le |
|---|---|---|

- Layer4
- ✓ UDP
- ESSYN
- SkypeCloud
- TCP Amp
- UDP-Lag
- Layer-7
- Source
- MIXED
- RUDY
- ARME
- GET
- HEAD
- POST
- Slowloris

## Booter Statistics

| | |
|---|---|
| Status: | Online |
| Total Users: | 1203 |
| Users Online: | 11 |
| Attacks Running: | 2/3 |

## User Statistics

| | |
|---|---|
| Boots Initiated: | 0 |
| Current IP: | 5.254.149.156 |
| Subscription Ends: | Free |
| Concurrent Attacks: | 1 attacks |
| Max Boot time: | 300 sec |

## Server Status

| | |
|---|---|
| Server Alpha [?]: | Available |

Question?
Click here to chat with us!

# 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

| Duration | Users | Victims | Attacks |
|---|---|---|---|
| Jan. 2013 - Mar. 2013 | 312 | 11,174 | 48,844 |

- 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




BLOG ADVERTISING

15 MAR 13 **The World Has No Room For Cowards**

Advertisement

## Details on the denial of service attack that targeted Ars Technica

Take a "booter" site survey, earn attacks like ones that targeted Ars, Brian Krebs.

by **Sean Gallagher** - Mar 18 2013, 5:20pm EST

HACKING NETWORKING 78

# TWBooter Details

- People
  - Askaa (Money)
  - DaL33t (Developer)
  - Both non-US citizens



# 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.

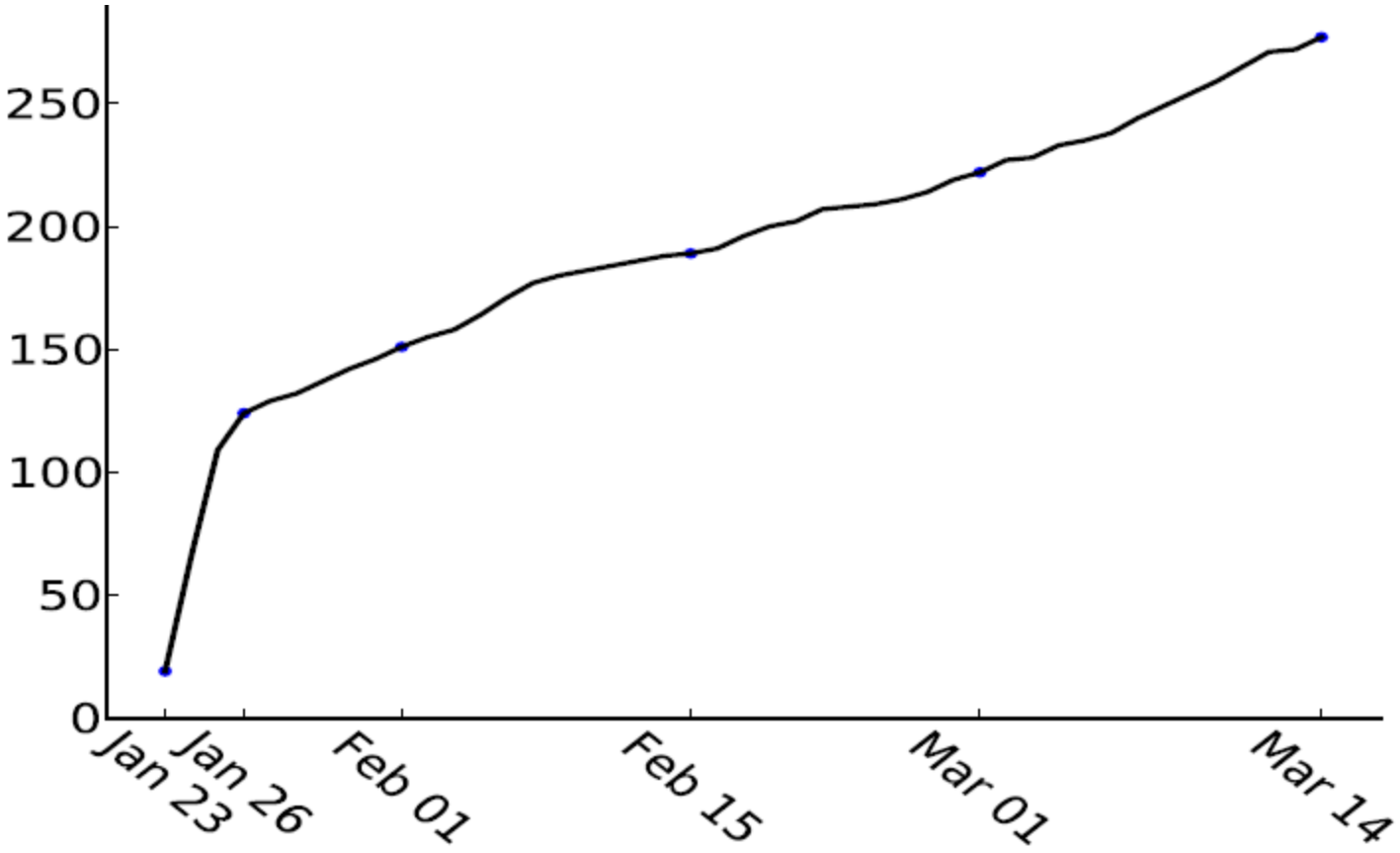
- SYN Floods spoof IP
- UDP Flood uses DNS amplification

| Attack Type | # of packets | Avg. packet size | Volume |
|---|---|---|---|
| UDP Flood | 4,552,899 | 1,363 bytes | 827 MBit/sec |
| SYN Flood | 5,625,086 | 54 bytes | 40 MBit/sec |

- 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.

| | Gamers | Website | Privileged |
|---|---|---|---|
| Number of users | 180 | 41 | 8 |
| Avg distinct targets per day | 3.32 | 3.46 | 2.86 |
| Avg attacks per day | 13 | 13 | 16 |
| Avg attack time per day | 59 m | 14 h | 105 h |

# 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 Angles police department

# Other Booter Services

- Leaks backend for Asylumbooter
  - 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



# Conclusion

- Booters focused on low cost ($10-$200) and usability
- Integrating features such as anti-cloudflare and Skype tracking
- Uses effective DNS amplification attacks
- TWBooter earned around $7,500/month