Booters
DDoS Attacks As A Paid Service

Jair Santanna
j.j.santanna@utwente.nl
Jairsantanna.com
My Goal:

Introduce **concept(s)** of DDoS attacks, its **evolution**, the **damage** caused by DDoS attacks, its current evolution phase (**booters**), and its **stakeholders**.
DDoS Attack
Distributed Denial of Service
Evolution:

Skilled Attackers

DoS Tools & Script-kiddies & Hacktivism
"Anonymous"

Booters, Stressers, DDoS-for-hire DDoS-as-a-Service

Hacker

Computer Scientist

#dSymp

dcypher Symposium 2017 | Oct 4th Media Plaza Utrecht | connects cybersecurity knowledge
#dSymp
dcypher Symposium 2017 | Oct 4th Media Plaza Utrecht | connects cybersecurity knowledge
How much damage would **YOU** (or other’s business) suffer?
Damage:

Triple-Play-Service

US$ 53,000,000


US$ 417,000,000

US$ 2,500,000,000
One single target can affect millions of victims!
+++Damage:

1.2 Tbits / second

108.49 Tbits / second

Booters

[4 years of investigation]
Online Exams!
Online Gamer
Booter (Simple) Ecosystem
Opportunity!
1. Booters are public!

2. Anyone can be a customer!

3. Booters rely on third-parties!
Research Question(s):

How to automatically find Booter Websites?
Paper: ”Bother Blacklist: Unveiling DDoS-for-hire Websites”
Crawler + Scraper + Classifier (+Machine Learn)

[botherblacklist.com]

#dSymp 
dcypher Symposium 2017 | Oct 4th Media Plaza Utrecht | connects cybersecurity knowledge
Security Essentials
SNT Helpdesk

Your email has not been sent. An technical problem has occurred. Please try again later, or contact your service desk.

The service desk would like you to be advised of the following:
Your computer has been quarantined because it was used to connect to known DDoS bootersites as well as connections from malware.

This system is probably compromised and being used by hackers. The system must be checked for hidden processes and hacker activities. It may even be necessary that the system must be reinstalled.

Please contact your service desk to reconnect your computer.

Contact Your Service Desk
Please use the form below to contact your service desk.

Name: Jair Santanna
Email address: j.santanna@utwente.nl
Message to the abuse department: What happened (again) with my machine?

Send message

User ID: ip(130.89.14.205)
QNET ID: 389243
Research Question(s):

How to automatically monitor users accessing booters?
Paper: "Bother List Generation: The Basis for Investigating DDoS-for-hire Websites"
Research Question(s):

How clients use booter attacks?
Paper: "Inside Booters: An Analysis on Operational Databases"
Research Question(s):

How to distinguish booters based on their attacks?
**Paper:** "Booters - An Analysis of DDoS-as-a-Service Attacks"

<table>
<thead>
<tr>
<th>#</th>
<th>Booter URL</th>
<th>Offer [Gbps]</th>
<th>Price [€]</th>
<th>Unique IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="http://booter.tw">http://booter.tw</a></td>
<td>?</td>
<td>10.90</td>
<td>8281</td>
</tr>
<tr>
<td>2</td>
<td><a href="http://restricted-stresser.info">http://restricted-stresser.info</a></td>
<td>5</td>
<td>1.95</td>
<td>7369</td>
</tr>
<tr>
<td>3</td>
<td><a href="http://anonymous-stresser.net">http://anonymous-stresser.net</a></td>
<td>5</td>
<td>3.12</td>
<td>6075</td>
</tr>
<tr>
<td>4</td>
<td><a href="http://destressbooter.com">http://destressbooter.com</a></td>
<td>25</td>
<td>3.89</td>
<td>4486</td>
</tr>
<tr>
<td>5</td>
<td><a href="http://flashstresser.net">http://flashstresser.net</a></td>
<td>?</td>
<td>3.89</td>
<td>3779</td>
</tr>
<tr>
<td>6</td>
<td><a href="http://dejabooter.com">http://dejabooter.com</a></td>
<td>10</td>
<td>3.89</td>
<td>2970</td>
</tr>
<tr>
<td>7</td>
<td><a href="http://rebel-security.com">http://rebel-security.com</a></td>
<td>Up to 3</td>
<td>3.00</td>
<td>281</td>
</tr>
<tr>
<td>8</td>
<td><a href="http://grimboot.com">http://grimboot.com</a></td>
<td>6</td>
<td>3.90</td>
<td>78</td>
</tr>
<tr>
<td>9</td>
<td><a href="http://quantumbooter.net">http://quantumbooter.net</a></td>
<td>1.5</td>
<td>8.00</td>
<td>54</td>
</tr>
<tr>
<td>10</td>
<td><a href="http://olympusstresser.org">http://olympusstresser.org</a></td>
<td>Up to 5</td>
<td>4.90</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td><a href="http://ebooter.5gbfree.com">http://ebooter.5gbfree.com</a></td>
<td>?</td>
<td>3.11</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td><a href="http://ydos.net">http://ydos.net</a></td>
<td>?</td>
<td>3.90</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td><a href="http://respamnet">http://respamnet</a></td>
<td>3</td>
<td>3.90</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td><a href="http://onionstresser.com">http://onionstresser.com</a></td>
<td>2</td>
<td>3.90</td>
<td></td>
</tr>
</tbody>
</table>

**€58,35**
CharGen-based attacks

DNS-based attacks

<table>
<thead>
<tr>
<th>DNS</th>
<th>Traffic Rate [Gbps]</th>
<th>Time [s]</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>0.4</td>
<td>0</td>
</tr>
<tr>
<td>NTP</td>
<td>0.8</td>
<td>0</td>
</tr>
<tr>
<td>CharGen</td>
<td>1.2</td>
<td>0</td>
</tr>
<tr>
<td>SSDP</td>
<td>1.6</td>
<td>0</td>
</tr>
</tbody>
</table>

\[ 108x \]

\[ 556.9x \]

\[ 358.8x \]
A red arrow points to a table with the following content:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Unique IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>8281</td>
</tr>
<tr>
<td>DNS</td>
<td>7369</td>
</tr>
<tr>
<td>DNS</td>
<td>6075</td>
</tr>
<tr>
<td>DNS</td>
<td>4486</td>
</tr>
<tr>
<td>DNS</td>
<td>3779</td>
</tr>
<tr>
<td>Chargen</td>
<td>2970</td>
</tr>
<tr>
<td>DNS</td>
<td>281</td>
</tr>
<tr>
<td>DNS</td>
<td>78</td>
</tr>
</tbody>
</table>

Another red arrow points to a website screenshot showing a list of resolver addresses, with one address highlighted in yellow: 9427x.
Research Question(s):

What are the third parties that (in)directly support booters operations?
Paper: "Quite Dogs Can Bite: What Booters We Should Go After? And Which Are Our Mitigation Options”

Taking Down Payment Accounts
Summary:

Booter (full) Ecosystem


#dSymp
Goal: “Introduce the concept(s) of DDoS attacks, its evolution, the damage caused by DDoS attacks, its current evolution phase (booters), and its stakeholders.”

Booters

DDoS Attacks As A Paid Service

Jair Santanna
j.j.santanna@utwente.nl
Jairsantanna.com