Millions of Targets Under Attack
a Macroscopic Characterization of the DoS Ecosystem

Mattijs Jonker†, A. King‡, J. Krupp§, C. Rossow§, A. Sperotto†, A. Dainotti‡
†University of Twente; ‡CAIDA, UC San Diego; §CISPA, Saarland University
Denial-of-Service (DoS) attacks

- Simple, yet effective class of attacks
- Have gained a lot in popularity over the last years
- Offered “as-a-Service” to the layman for only a few USD
We aim at presenting a large-scale longitudinal analysis of the DoS ecosystem by means of a macroscopic characterization of attacks, attack targets, and DDoS Protection Services.
Data sets

- Four global Internet measurement infrastructures
  - A large network telescope
  - Logs from amplification honeypots
  - Data from large-scale, active DNS measurements
  - A DNS-based data set focusing on DDoS Protection Services (DPS) usage
UCSD Network Telescope

• A /8 darknet

• Captures DoS attacks with randomly (and uniformly) spoofed IP addresses

• Captures ~1/256th of IPv4 address space

• Any sizable attack should be visible
Amplification honeypot (AmpPot)

- Honeypot that mimicks reflectors
  - various protocols (e.g., NTP, DNS, and CharGen)
- Tries to be appealing to attackers
  - i.e., by offering large amplification
- Twenty-four AmpPot instances
  - Geographically & logically distributed
Amplification honeypot (AmpPot)

1. DNS request
   - Src: 10.0.0.17
   - Dst: 192.168.0.1

2. Collect

Attacking host (e.g., botnet slave)

Amplification honeypot
- IP: 192.168.0.1

Victim
- IP: 10.0.0.17
Attack events coverage

- We analyze two years of attack traces
  - March 1, 2015 – Feb 28, 2017
- The attacks data sets complement each other:
  - honeypots don’t register randomly spoofed attacks
  - a darknet doesn’t register reflection attacks
Attacks analysis

<table>
<thead>
<tr>
<th>source</th>
<th>#events</th>
<th>#targets</th>
<th>#/24s</th>
<th>#ASNs</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCSD-NT</td>
<td>12.47M</td>
<td>2.45M</td>
<td>0.77M</td>
<td>25990</td>
</tr>
<tr>
<td>AmpPot</td>
<td>8.43M</td>
<td>4.18M</td>
<td>1.72M</td>
<td>24432</td>
</tr>
<tr>
<td></td>
<td>20.90M</td>
<td>6.34M</td>
<td>2.19M</td>
<td>32580</td>
</tr>
</tbody>
</table>

- We observe almost 21 million attacks over 2 years
  - average of 30k daily
- 2.19 million /24s observed
- This number is about a third of recent estimates of the actively used IPv4 address space\textsuperscript{1,2}

\textsuperscript{1} Sebastian Zander et al. Capturing Ghosts: Predicting the Used IPv4 Space by Inferring Unobserved Addresses. In IMC’14.
\textsuperscript{2} Philipp Richter et al. Beyond Counting: New Perspectives on the Active IPv4 Address Space. In IMC’16.
Attacks analysis

<table>
<thead>
<tr>
<th>reflector</th>
<th>events (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP</td>
<td>40.08</td>
</tr>
<tr>
<td>DNS</td>
<td>26.17</td>
</tr>
<tr>
<td>CharGen</td>
<td>22.37</td>
</tr>
<tr>
<td>SSDP</td>
<td>8.38</td>
</tr>
<tr>
<td>RIPv1</td>
<td>2.27</td>
</tr>
<tr>
<td>Other</td>
<td>0.73</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP proto</th>
<th>TCP</th>
<th>UDP</th>
<th>ICMP</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>events (%)</td>
<td>79.4</td>
<td>15.9</td>
<td>4.5</td>
<td>0.2</td>
</tr>
</tbody>
</table>

- NTP is the most-abused protocol in reflection and amplification attacks
- TCP is the most prominent IP proto in randomly spoofed attacks
### Attacks analysis

<table>
<thead>
<tr>
<th>service</th>
<th>events (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>48.68</td>
</tr>
<tr>
<td>HTTPS</td>
<td>20.68</td>
</tr>
<tr>
<td>MySQL</td>
<td>1.12</td>
</tr>
<tr>
<td>DNS</td>
<td>1.07</td>
</tr>
<tr>
<td>Other</td>
<td>28.45</td>
</tr>
</tbody>
</table>

- We map dst:port in randomly spoofed attacks to services using IANA assignments.
- Our results show that almost 70% (potentially) target Web infrastructure.
Active DNS measurement data

- Third data set: active DNS measurements
- Contains, among others, A records (i.e., IPv4 address)
  - allows historical address lookups
- We use data for all domains under .com, .net, and .org
  - Together comprise ~50% of global DNS namespace
Active DNS measurement data

- Used to map IP addresses to Web sites
- We consider the presence of a www. in the DNS a Web site
  - We find 210 million such Web sites over two years

<table>
<thead>
<tr>
<th>start</th>
<th>end</th>
<th>zone</th>
<th>#Web sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-03-01</td>
<td>2017-02-28</td>
<td>.com</td>
<td>173.7M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.net</td>
<td>21.6M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.org</td>
<td>14.7M</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>210.0M</strong></td>
</tr>
</tbody>
</table>
Attacks Web site association over time

- 572k of 6.34M target IPs host 1 or more Web site
- 134M Web sites associated with attacks over 2y
  - That is 64% of the overall 210M observed
  - average is ~4M daily (3%)
- Peaks correspond to large hosters under attack
  - up to 15M Web sites associated
Use of DDoS Protection Services (DPS)

- We study if attacks on Web sites affect DPS migration
- DPS are commercial, cloud-based mitigation services
- We cover 9 leading commercial providers:
  - Akamai, CenturyLink, CloudFlare, DOSArrest, F5, Incapsula, L3, Neustar & Verisign
- ... and one smaller DPS:
  - VirtualRoad – protects freedom of speech organizations
- 33 million Web sites (24.6% of attacked Web sites)
Classification of Web sites

- com, net, org (210M)
  - Attack Observed (134M (64%))
    - Preexisting Customer (24.9M (18.6%))
      - Migrating (4.7M (4.31%))
    - Non-preexisting Customer (109M (81.3%))
      - Non-Migrating (104M (95.4%))
  - No Attack Observed (76M (36%))
    - Preexisting Customer (0.67M (0.89%))
      - Migrating (2.5M (3.32%))
    - Non-preexisting Customer (75.3M (99.1%))
      - Non-Migrating (72.8M (96.7%))
Migration delay

Earlier migration follows attacks of higher intensity
Conclusions

• Proved the potential of large-scale longitudinal characterization of the DoS ecosystem
  – A third of actively used /24s under attack
  – A prevalence towards attacks that target Web infrastructure port
  – About two thirds of Web sites involved in attacks
  – A correlation between attack intensity and DPS migration
Questions?

Mattijs Jonker
m.jonker@utwente.nl