DDos Prevention and Mitigation
Friday, 21 October 2016

http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

http://downdetector.com/
Denial-Of-Service 101

• What?
  - Attack on IT infrastructure
  - Make machine/network resource unavailable
  - Temporary or indefinite
  - Not a new invention!
Denial-Of-Service 101

• How?
  - Crashing service
  - Flooding service

• Effect
  - Prevent legitimate users to be serviced
Denial-Of-Service 101

• **Targets:**
  - Usually high-profile sites
  - But not only

• **Initiators**
  - Hackers
  - Script kids
  - Criminals
  - State actor
  - Insider
Denial-Of-Service 101

- Costs
  - Mitigation costs
  - Lost revenue
  - Reputation
Special Forms Of DOS

• Distributed DOS
  - Involving multiple devices in the attack

• APDOS
  - Involving an advanced persistent thread
  - Requires resources and sophistication

• DOS as a service
  - Entry barrier is getting lower
  - Growing market

DDoS Attack Classes

• TCP Connection Attack
  - Intention to use up available connections

• Volumetric Attack
  - Intention to cause congestions

• Fragmentation Attack
  - Intention to overwhelm request handling

• Application Attack
  - Intention to exploit specific aspects of an application
DDoS Amplification

- DNS Reflection
  - Small request, big response

- Chargen Reflection
  - Streams of random characters on demand
Statistics on DDoS

More than 2000 daily DDoS Attacks are observed worldwide by Arbor Networks.

ATLAS Threat Report

1/3 of all downtime incidents are attributed to DDoS attacks.

Verisign/Merril Research

http://www.digitalattackmap.com/

DDoS attacks, Q2 2016 vs. Q2 2015
129% increase in total DDoS attacks
151% increase in infrastructure layer (layers 3 & 4) attacks
276% increase in NTP reflection attacks (a record high)
70% increase in UDP flood attacks

State of the Internet Security Report by Akamai
Statistics on DDoS

Top 10 Source Countries for DDoS Attacks, Q2 2016

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>56.09%</td>
</tr>
<tr>
<td>US</td>
<td>17.38%</td>
</tr>
<tr>
<td>Taiwan</td>
<td>5.22%</td>
</tr>
<tr>
<td>Canada</td>
<td>3.77%</td>
</tr>
<tr>
<td>Vietnam</td>
<td>3.70%</td>
</tr>
<tr>
<td>Brazil</td>
<td>2.96%</td>
</tr>
<tr>
<td>Spain</td>
<td>2.94%</td>
</tr>
<tr>
<td>Singapore</td>
<td>2.90%</td>
</tr>
<tr>
<td>Italy</td>
<td>2.65%</td>
</tr>
<tr>
<td>UK</td>
<td>2.38%</td>
</tr>
</tbody>
</table>

DDoS Attack Frequency by Industry

State of the Internet Security Report by Akamai
DDoS Prevention

• Keep your software up-to-date

• Know your network and services
  - Make inventory on a regular basis
  - Monitor

• Don’t make enemies and avoid becoming a target
DDos Prevention

• Recommendations by the Dutch government
  - Make an overview and monitor your infrastructure
  - Check with each of your third-party suppliers to find out which (D)DoS countermeasures are in place and what the relevant contractual agreements are
  - Find out which countermeasures have been taken to protect your in-house infrastructure and take additional steps, if necessary
  - **Prepare your incident response** and think about **failover** scenarios for your online services
  - **Prepare a communication strategy**
DDoS Prevention

- Ingress filtering (BCP38)
- RPKI
- BGPSEC
DDoS Mitigation

- Detection!!!
  - You need to be able to detect an attack
  - Popular service vs. attack

![Memory usage - by day](image)
DDos Mitigation

- BGP blackholing
DDos Mitigation

- Traffic Scrubbing
  - Services like NaWas

DDos Mitigation

• Spread the word and inform the right people
  - Abuse-c
  - National CERTs
  - Affected companies
DDos Mitigation

- Spread it even further
- Working Group mailing list
  - Routing WG
  - Anti-Abuse WG
- NOG/National lists
  - NANOG
  - NLNOG, DENOG, PLNOG, SWINOG, etc.
  - MKNOG?
Questions
christian.teuschel@ripe.net
@cteuschel