Anti-DDOS (at) RedIRIS

Francisco Monserrat

Connecting Spanish R&D&i since 1988
DDOS a new security problem?
Denial-of-service attack

From Wikipedia, the free encyclopedia

"DoS" redirects here. For the family of computer operating systems, see DOS. For the United States federal executive department, see United States Department of State. For other uses, see DOS (disambiguation).

In computing, a denial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[1]

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.

A DoS or DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, disrupting trade.
Has your organization received a Denied of Service (DOS) attack in the last year?
Why we care about DDOS?

Collateral damage

From Wikipedia, the free encyclopedia

For other uses, see Collateral damage (disambiguation).

The examples and perspective in this article deal primarily with the United States and do not represent a worldwide view of the subject. You may improve this article, discuss the issue on the talk page, or create a new article, as appropriate. (March 2018) (Learn how and when to remove this template message)

Collateral damage is the deaths, injuries, or other damage inflicted on an unintended target. In American military terminology, it is used for the incidental killing or wounding of non-combatants or damage to non-combatant property during an attack on a legitimate military target.[1][2] In US military terminology, the unintentional destruction of allied or neutral targets is called friendly fire.
Volumetric (data volume) attacks
Non volumetric attacks
Non volumetric attacks

Graph Type: Stacked

Customer: UAM
Description: Universidad Autónoma de Madrid

<table>
<thead>
<tr>
<th>Application</th>
<th>IN (Kpps)</th>
<th>OUT (Kpps)</th>
<th>TOTAL (Kpps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssl</td>
<td>66.98</td>
<td>55.03</td>
<td>122.01</td>
</tr>
<tr>
<td>http</td>
<td>36.68</td>
<td>23.95</td>
<td>60.63</td>
</tr>
<tr>
<td>other UDP</td>
<td>17.68</td>
<td>13.71</td>
<td>31.39</td>
</tr>
<tr>
<td>other TCP</td>
<td>6.80</td>
<td>6.53</td>
<td>13.33</td>
</tr>
<tr>
<td>macromedia-fcs</td>
<td>1.24</td>
<td>1.18</td>
<td>2.42</td>
</tr>
<tr>
<td>dns</td>
<td>697.00</td>
<td>615.00</td>
<td>1.31 Kpps</td>
</tr>
<tr>
<td>xmpp</td>
<td>283.00</td>
<td>266.00</td>
<td>549.00</td>
</tr>
<tr>
<td>nntps</td>
<td>0.00</td>
<td>399.00</td>
<td>399.00</td>
</tr>
<tr>
<td>telnet</td>
<td>228.00</td>
<td>16.00</td>
<td>244.00</td>
</tr>
<tr>
<td>quake3</td>
<td>0.00</td>
<td>188.00</td>
<td>188.00</td>
</tr>
<tr>
<td>qq</td>
<td>79.00</td>
<td>83.00</td>
<td>162.00</td>
</tr>
<tr>
<td>imap</td>
<td>97.00</td>
<td>24.00</td>
<td>121.00</td>
</tr>
<tr>
<td>ssh</td>
<td>0.00</td>
<td>79.00</td>
<td>79.00</td>
</tr>
<tr>
<td>sip</td>
<td>0.00</td>
<td>79.00</td>
<td>79.00</td>
</tr>
<tr>
<td>rdp</td>
<td>23.00</td>
<td>19.00</td>
<td>42.00</td>
</tr>
<tr>
<td>ldap</td>
<td>39.00</td>
<td>0.00</td>
<td>39.00</td>
</tr>
<tr>
<td>ntp</td>
<td>39.00</td>
<td>0.00</td>
<td>39.00</td>
</tr>
<tr>
<td>stun</td>
<td>39.00</td>
<td>0.00</td>
<td>39.00</td>
</tr>
<tr>
<td>rip</td>
<td>39.00</td>
<td>0.00</td>
<td>39.00</td>
</tr>
<tr>
<td>rtsp</td>
<td>16.00</td>
<td>0.00</td>
<td>16.00</td>
</tr>
<tr>
<td>pop</td>
<td>0.00</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>emule</td>
<td>0.00</td>
<td>1.00</td>
<td>1.00</td>
</tr>
</tbody>
</table>

Graph Title: Peakflow SP: Customer 'UAM' All Applications

Graph Description: Period: Today Start: 24 hours ago End: now Units: pps
Non volumetric attacks

The Internet of ransomware things...

- **Hungry? Pay up and I'll unlock my door!**
- **On strike until you send money to my hackers.**
- **20 bucks in my PayPal account or I'll only brew Decaf!**
- **I'll be burning the toast if you don't get me some dough!**
- **If you don't send us cash, your reputation will be in the trash.**
- **Wire my hacker $100 or I'll reverse my motor and blow dirt all over this place!**
- **Your dirty dishes can wait, I'm busy mining Bitcoins.**
- **I'll start your car, but only to take you to your bank to make a transfer.**
- **I'll tell everyone on your social network that you were stupid enough to buy an internet-connected broom!**
- **Send me $25 or I'll tell everyone on your social network that you were stupid enough to buy an internet-connected broom!**
- **The next time you leave, it'll cost you $100 bucks to get back into the house, unless you give me $75 now!**
- **My alarm system is going to go off randomly throughout the night, unless you "donate"."
How do you detect a DOS?

- Social media, 
  📲  📱
- SIEM correlation
- User calling
- Outside call
- Post Morten analysis
Network information
Mitigation & cure

**cured; curing**

**Definition of cure (Entry 2 of 3)**

*transitive verb*

1. a : to restore to health, soundness, or normality
   // cured him of a rare blood disease

2. a : to deal with in a way that eliminates or rectifies
   // ... his small size, which time would cure for him ...
   — William Faulkner

   b : to free from something objectionable or harmful
   // trying to cure him of a bad habit

**mitigate**

*transitive verb*

1. : to cause to become less harsh or hostile : MOLLIFY
   // aggressiveness may be mitigated or ... channeled
   — Ashley Montagu

2. a : to make less severe or painful : ALLEVIATE
   // mitigate a patient's suffering

   b : EXTENUATE
   // attempted to mitigate the offense
Blackhole
FlowSpec filtering
Scrubbing center
Scrubbing Center

Centro de mitigación principal

Centro de mitigación secundario

Router

Switch

Mitigador/Limpiador 100Gb

Conexiones 100Gbps

Canal óptico de 10/100Gbps dedicado

Conexiones 10Gb

Conexiones 10Gbps

Conexiones 10/100Gbps

Conexiones 10/100Gbps

Incoming DDOS traffic

Incoming DDOS traffic

Conexiones 10/100Gbps

Red IRIS
Timeline

Q1-18
- Tener launched

Q2-18
- New system deployment

Q1-19
- Advanced guarantee
- Visualization tender
- Flowspec testing

Q2-20
- End of advanced guarantee
- Visualization deployment
- Flowspec service
THANK YOU VERY MUCH!