Cost Effective Ways to Handle a Distributed Denial of Service Attack (Non-fiction)

Presented by:
Tim Rettig
President
Tim.Rettig@intrustgroup.com
Objectives

- Learn what a Distributed-Denial of Service (DDoS) attack is.

- Learn some cost-effective ways to reduce the effects of a DDoS attack.
Speaker Info

Tim Rettig
President
INTRUST GROUP

Tim.Rettig@intrustgroup.com
(513) 842-3160
http://www.intrustgroup.com
http://blog.timrettig.com
http://www.linkedin.com/in/timrettig
What is a DDoS Attack?
**DDoS**

- Distributed Denial of Service Attack
  - A large number of computers in multiple locations send either regular or malicious traffic at a victim.
How to get a Botnet

1. 
2. 
3. 
4.
### Some Known Botnets

<table>
<thead>
<tr>
<th>Date created</th>
<th>Name</th>
<th>Estimated no. of bots</th>
<th>Spam capacity</th>
<th>Aliases</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009 (May)</td>
<td>BredoLab</td>
<td>30,000,000</td>
<td>3.6 billion/day</td>
<td>Oficla</td>
</tr>
<tr>
<td>2008 (around)</td>
<td>Mariposa</td>
<td>12,000,000</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>?</td>
<td>Conficker</td>
<td>10,500,000+</td>
<td>10 billion/day</td>
<td>DownUp, Kido</td>
</tr>
<tr>
<td>?</td>
<td>Zeus</td>
<td>3,600,000</td>
<td>?</td>
<td>Gorhax, Kneber</td>
</tr>
<tr>
<td>2007 (Around)</td>
<td>Cutwail</td>
<td>1,500,000</td>
<td>74 billion/day</td>
<td>Pandex, Mutant</td>
</tr>
<tr>
<td>?</td>
<td>Grum</td>
<td>560,000</td>
<td>39.9 billion/day</td>
<td>Tedroo</td>
</tr>
<tr>
<td>?</td>
<td>Mega-D</td>
<td>509,000</td>
<td>10 billion/day</td>
<td>Ozdok</td>
</tr>
<tr>
<td>?</td>
<td>Kraken</td>
<td>495,000</td>
<td>9 billion/day</td>
<td>Kracken</td>
</tr>
<tr>
<td>2007 (March)</td>
<td>Srizbi</td>
<td>450,000[1]</td>
<td>60 billion/day</td>
<td>Cbeplay, Exchanger</td>
</tr>
<tr>
<td>?</td>
<td>Lethic</td>
<td>260,000</td>
<td>2 billion/day</td>
<td>None</td>
</tr>
<tr>
<td>....</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Case Study Victim

Life Insurance for Funeral Funding
Called INTRUST
Cloud Hosting

- Load Balancers
- Cloud Servers
- Dedicated Servers
- Cloud Storage
Cloud Costs

- CPU and Bandwidth cost about $100/day
Interesting Article

Black Hat: Will New Breed of DOS Attacks Make Cloud Unaffordable?

By William Jackson  •  01/20/2011

The cloud is the current Next Big Thing in computing, and the Next Big Thing in attacks could be a new breed of economic denial-of-service attacks intended to use up resources and drive up the cost of cloud computing, warns a senior security researcher at Adobe Systems.

"DOS is the next battleground," Bryan Sullivan said Wednesday at the Black Hat Federal conference being held in Arlington, Va. "That's where the future is going."

The new generation of attacks described by Sullivan operate high in Layer 7, the application layer of the Open Systems Interconnection model, and target specific lines of code in a specific application. Although the impact is less widespread than a traditional Layer 4 distributed DOS attack using the resources of a botnet, it is highly targeted and effective. A single HTTP request of several hundred bytes could crash a server.

Next Try: DDoS Specialists

- Moved website to their server
  - Site stayed up, but was a little slow
- Company quoted $1,500/month for hosting
Next Try: Cloud Server

- Virtual Server with 100Mbps pipe
- Cost: $150/month
Next Try: Added GeoDNS

Web Server

Authoritative DNS Server

domainname.com

IP Address
GeoDNS Implementation

- Dropped TTL to 5 minutes
- Used SimpleDNS with GeoDNS plug-in
- Limitations:
  - Geo IP address database accuracy
  - DNS server of clients
- Hosted solutions:
Additional Mitigation Tactics

- Switching site to text only reduced bandwidth and CPU cycles.
- Firewalling subnets of attacking computers helped keep site online.
  - Netstat
  - Look for IP addresses with multiple connections
  - Perform network whois on IP address
  - Add subnet to firewall
  - Repeat
Firewalling Fun
The FBI Meeting
IIS 7.0 Mitigation Strategy
Installed Dynamic IP Restrictions

- http://www.iis.net/download/DynamicIPRestrictions
To prevent the server from running out of memory, set all application pools to recycle more frequently.
Limit bandwidth on website accordingly.
Summary

- By combining the cloud-hosted server, GeoDNS, and Dynamic IP restrictions on IIS, we were able to keep the site operating.

- First attack lasted about eight days, a second attack a month later lasted about five days.
About INTRUST GROUP
We are the IT department for many organizations.

- Remote/Onsite Help Desk Support
- Proactive Server/Desktop Monitoring
- IT Management, Consulting & Projects
- Website Design
- Cloud Services
- Offices in Chicago and Cincinnati
- Founded in 1992
Clients

- Private Companies $5 Million to $1 Billion+
- Schools
- Universities
- Utility Companies
- Government Agencies
- Police Departments
- Fire Departments
Is this your support challenge?

Data Center Colo

Mobile users

Cloud Services

Headquarters

Your Remote Offices
One support company.
One fixed, monthly cost.
User Support
IT Management
Stop by our table today for more information.

Please allow us to delight you.
Questions/Discussion

Tim.Rettig@intrustgroup.com
(513) 842-3160