Distributed Denial of Service
War Stories from the Cloud Front

Michael Smith
Security Evangelist
Agenda

- Akamai and DDOS
- Threats and Capabilities
- Fail Patterns
- July 4th, 2009
- Building Defenses
- Summary
The Akamai Cloud: Largest Distributed Computing Platform in the World

- 73,000+ Servers
- 1,600+ Locations
- 70 Countries

- All branches of the US Military
- 85 of the top 100 online retailers
- 9 of the top 10 virus companies
- 29 of the top 30 M&E companies

- 4.5+ Tbps, 15-25% of web traffic
- 10+ Million transactions per second
Akamai Topology and DDoS

- Geographic Dispersion
- Traffic Management
- Device Offload
- Blocking
- Site Failover

Securing a Better Internet

© 2010 Akamai
Agenda

✓ Akamai and DDOS
✓ Threats and Capabilities
✓ Fail Patterns
✓ Building Defenses
✓ July 4th, 2009
✓ Active Response
✓ Summary
Threats: Extortion

“You have a nice website, it would be a shame if anything were to happen to it. $30,000 can buy you an insurance policy to keep that from happening.”
Threats: State-Sponsored

- Estonia
- Georgia
- United States

Or were they?
Threats: Activists/Protestors
Greetings, Anonymous

Our beloved Pirate Bay has been recently taken down by certain Media Interests groups. It's back up, but-
It has happened far too many times.
It is time to show a clear message to those that wish to harm our Internet Refuge.
It is time to strike back.
We must show these jerks what we think of their games.
We can not let them win.
We must retaliate.

Our first objective was to take down Aiplex, the ones that DDoSed The Pirate Bay.
Everything had went even better than expected.
We selected a new target, MPAA, in just eight minutes after launching the attack, their website suffered a tremendous blow at the hands of Anonymous.

Instead of selecting another target we will be launching a second attack against the MPAA on September 19th, 3:00PM.
This is to show these corporate jerks that we won't stand for them messing with our websites.
If you do not use TPB, remember that Private Trackers are the next target.
So, if you are still with me, Lets give them a night to remember.
Let this be a lesson to you, kids: If you're dumb enough to get caught cheating in SOCOM, you're probably dumb enough to get caught using a botnet to launch a DDOS attack against PlayStation.com. --Escapist Magazine

Securing a Better Internet
Peak Attack Traffic per year

- 2001: 0.4 Gbps
- 2002: 1.2 Gbps
- 2003: 2.5 Gbps
- 2004: 10 Gbps
- 2005: 17 Gbps
- 2006: 24 Gbps
- 2007: 40 Gbps
- 2008: 49 Gbps

(Arbor Networks)
Peak Attack Traffic per year

- 2001: 0.4 Gbps
- 2002: 1.2 Gbps
- 2003: 2.5 Gbps
- 2004: 10 Gbps
- 2005: 17 Gbps
- 2006: 24 Gbps
- 2007: 40 Gbps
- 2008: 49 Gbps
- July 4th, 2009: 124 Gbps (Akamai)

Source: Arbor Networks
Agenda

✓ Akamai and DDOS
✓ Threats and Capabilities
✓ Fail Patterns
✓ July 4th, 2009
✓ Building Defenses
✓ Summary
Fail Patterns: Network and Devices

- Includes circuits, firewalls, WAFs, load balancers
- Flooding Attacks (attacker bandwidth > you)
  - UDP
  - SYN (also OS)
  - ICMP (ping -f)
  - Reflected Attacks
- Web Objects (small request, large response)
  - Images and movies (yes, pr0nz too)
  - Documents (.doc .pdf .xls)
  - Zip files
  - Downloadable software
- If the network is attacked, everything on that network fails (shared Internet connections)
Fail Patterns: DNS

- DNS is a Single Point of Failure—all other traffic dies
- DNS is UDP is bad
- Limited to 10 nameservers per domain
- DNSSEC creates network, application, and OS load <oops>
Fail Patterns: Mail Servers

- Filtering email creates server and application load
- Requires large amounts of attacker bandwidth
- Email can have large attached objects
- Fail:
  - Mailbox size limits
  - Storage
  - Processing power for filters
Fail Patterns: Web and App Servers

- Load large objects
- Exercise business logic
- Siege [http://www.joedog.org/index/siege-home](http://www.joedog.org/index/siege-home)
- Shell scripts work:
  - while true;
  - wget [http://www.mpaa.org/Resources/86fec176-1e62-401c-aaa6-e58c4078426e.jpg](http://www.mpaa.org/Resources/86fec176-1e62-401c-aaa6-e58c4078426e.jpg) &
  - wget [http://www.mpaa.org/Resources/ccb46057-c90e-4770-9f81-dd16b82ec062.jpg](http://www.mpaa.org/Resources/ccb46057-c90e-4770-9f81-dd16b82ec062.jpg) &
  - wget [http://www.mpaa.org/Resources/3d434c12-7569-45b0-a242-2ca0be1036d6.jpg](http://www.mpaa.org/Resources/3d434c12-7569-45b0-a242-2ca0be1036d6.jpg) &
  - ...
  - done
Fail Patterns: Database Servers

- while true;
- do wget 'http://riaa.com/goldandplatinumdata.php?table=SEARCH_RESULTS&title=&artist=&label=&format=&category=&type=&awardDescription=&startMonth=1&startYear=0&endMonth=12&endYear=2009&sort=Date&sense=ASC&perPage=5000000000&go=Search' > /dev/null &
- done
Agenda

✓ Akamai and DDOS
✓ Threats and Capabilities
✓ Fail Patterns
✓ July 4th, 2009
✓ Building Defenses
✓ Summary
### July 4th DDoS Attack

<table>
<thead>
<tr>
<th>Top Targets</th>
<th>Peak Traffic</th>
<th>Times Above Normal Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>US Government 1</td>
<td>124 Gbps</td>
<td>598x</td>
</tr>
<tr>
<td>US Government 2</td>
<td>32 Gbps</td>
<td>369x</td>
</tr>
<tr>
<td>Financial 1</td>
<td>26 Gbps</td>
<td>110x</td>
</tr>
<tr>
<td>US Government 3</td>
<td>9 Gbps</td>
<td>39x</td>
</tr>
<tr>
<td>US Government 4</td>
<td>9 Gbps</td>
<td>19x</td>
</tr>
<tr>
<td>US Government 5</td>
<td>2 Gbps</td>
<td>9x</td>
</tr>
<tr>
<td>US Government 6</td>
<td>1.90 Gbps</td>
<td>6x</td>
</tr>
<tr>
<td>US Government 7</td>
<td>0.73 Gbps</td>
<td>*</td>
</tr>
</tbody>
</table>

OC-192 speed is ~10Gbps at $2M/month (GSA rates for TIC)

Source: Akamai

* Site down before Akamai
July 4th DDoS Attack Timeline

14:00
Alert fires in Akamai’s Network Operations and Command Center
July 4th DDoS Attack Timeline

16:00
Continued elevated traffic.
Customer notification initiated based on SOP.

200 Mbps
Normal traffic level

5,000 Mbps
Elevated traffic level
July 4th DDoS Attack Timeline

20:00 Attack increases rapidly

- Attack Size: Gbps
- Probes

0:00 8:00 16:00 0:00 8:00 16:00

July 4th, 2009

July 5th, 2009
July 4th DDoS Attack Timeline

21:00 Akamai Identifies Sources

97,882 Unique IP’s in 30 mins
July 4th DDoS Attack Timeline

23:00 Mitigation measures started

22:50 125 Gbps
Peak bandwidth

23:50 795K
Peak page views
July 4th DDoS Attack Timeline

23:00 Mitigation measures started

Few common attackers between spikes. Only 4,284 IP’s Shared Across all Spikes.
July 4th DDoS Attack Timeline

23:00 Mitigation measures started

Few common attackers between spikes. Only 4,284 IP’s Shared Across all Spikes.
July 4th DDoS Attack Timeline

0:30 Block Korean traffic

Attack Size - Gbps

0:00 8:00 16:00 0:00 8:00 16:00

July 4th, 2009
July 5th, 2009
July 4th DDoS Attack Timeline

9:30
Quarantine Korea traffic to isolated infrastructure
Attacks focused on two sites.

- July 5th – Attacks spread to include 5 other sites. Even traffic spread.
- July 5th (late) – Attack shifts bulk of attack to 2 new sites.
- July 6th (late) – Attack Ends.
Observations

- Attacks are sophisticated
- Attacks are long: 3 Day Duration
- Attacks are large:
  - 300,000+ Attack IPs
  - 7+ Billion Total Page Views
  - 200+ Tbytes
  - Equal to 50 STM16 and 2,500 Servers
- Attacks are fast:
  - Traffic to a single site reached 100 Gbps in just four hours
Agenda

- Akamai and DDOS
- Threats and Capabilities
- Fail Patterns
- July 4th, 2009
- Building Defenses
- Summary
Defense: Basic Strategies

- Monitoring
- Tuning
- Caching
- Filtering
- Traffic Management
Defense: Instrumentation and Monitoring

- Percentage of total network capacity
- Percentage of total OS/DB load
- Increase of 50% of traffic in 8 hours
- Increase of 50% of traffic over historical average
- Percentage of “bizarre user agent strings”
- Server response times
- Increase in error responses

“Is it an actual attack or an awesome marketing campaign, and does it matter?”
Defense: Communications and Escalation

- Attackers pick inconvenient times
- Similar to DR/COOP plans
- Authority to activate SOP given to NOCC teams
- Established “red button” to DDoS plan
  - 5% of traffic through DDoS system
  - DNS switch to activate
Defense: Caching and Dispersion

Customer Webserver

HTTP TTL
HTML Pragmas
CDN Configuration

End User
Defense: Application, Web, DB Servers

- Tuning means higher throughput and better user experience
- Input validation doesn’t just mean XSS and SQLi
  - User-supplied query limits
  - User-supplied workloads (&action=)
  - Validate input based on “business logic” or “context”
- In-application caches
- Communication with upstream filtering/caching
Defense: Low-Bandwidth Site

- Low-bandwidth sites can be cached or served from a cloud or alternate site
- Google for standard downloadable files:
- Google image search: site:targetsitet.com &imgsz=medium|large|xlarge
- Web analytics tools can find large objects
- Can you use your mobile site?
Defense: Traffic Redirect

- Rewrite the target url to the redirect method
- Redirect:
  - Page only with JavaScript
  - 302 codes (small)
- Rewrite the “landing url” to the real page
- Redirects and redirect pages can be cached!
- Very easy for the attacker to manually retarget
Defense: HTTP Traffic Filtering

- UserAgent
- Accept-Language
- Cookie set by site
- Cookie set by client-side JavaScript
- Referrer
- All of these together
Defense: DNS

- Make DNS resilient
  - Multiple servers behind a VIP
  - Geographic dispersion
- DNS resolution by geography
- Direct % of traffic to low-bandwidth or alternate hosting
- Blackhole attack traffic to 127.0.0.1
- Quarantine servers
Defense: Email

- Maximum attachment size
- GreetPause
- Use DNS to blackhole regions
Defense: Network Traffic Scrubbers/Filters

- Filter by IP, CIDR, ASN, or country
- Drop Layer 3-5 attack traffic
- Organic to Content Delivery Networks
- Services provided by ISPs
- Offload of attack traffic to places outside of your network
- Hiding the target servers to force traffic through the scrubbers/filters
Defense: Waiting Room

- Uses load.txt to notify CDN of resource overload
- Low-bandwidth site residing on the edge
- Sets a cookie on the client
  - One value gets sent to origin
  - One value stays in queue
- Incrementally migrates users to origin servers as capacity is decreased
Agenda

- Akamai and DDOS
- Threats and Capabilities
- Fail Patterns
- July 4th, 2009
- Building Defenses
- Summary
Summary: Defending Yourself

- What is the “cost” for an outage? (impact)
  - Income
  - Brand Preservation
  - Loss of Confidence
  - Timeliness of Attack
  - Use DR/COOP Figures
- How much of a target are you (frequency)
- Priorities for protection (risk management)
Agenda

- Akamai and DDOS
- Threats and Capabilities
- Fail Patterns
- July 4th, 2009
- Building Defenses
- Summary