How to Survive DDoS
The Play at Home Game

Michael Smith mismith@akamai.com
Security Evangelist
The Akamai Cloud: Largest Distributed Computing Platform in the World

- 100,000+ Servers
- 2,400+ Locations
- 70 Countries
- All branches of the US Military
- 95 of the top 100 online retailers
- 9 of the top 10 anti-virus companies
- 29 of the top 30 M&E companies
- 4.5+ Tbps, 15-25% of web traffic
- 16+ Million transactions per second
What We’ll Cover

- Traffic Samples
- Prepare
- Detect
- Respond
- Post-Incident
Traffic Sample: SYN Flood

SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
Traffic Sample: Simple Bot

SYN
ACK
SYN-ACK

GET / HTTP 1.1
RST
RST
RST
RST
Traffic Sample: LOIC 1.1.2.3

SYN

ACK

SYN-ACK
  Get / HTTP/1.1
  HOST: www.targetsite.com
  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)

RST

RST

RST

RST
Traffic Sample: Tor’s Hammer

POST / HTTP/1.1
Host: localhost
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; FDM; .NET CLR 2.0.50727; InfoPath.2; .NET CLR 1.1.4322)
Connection: keep-alive
Keep-Alive: 900
Content-Length: 10000
Content-Type: application/x-www-form-urlencoded

gsl6
Traffic Sample: Bitcoin Miner

GET / HTTP/1.1
Host: www.targetsite.com
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Accept-Charset: utf-8;q=0.7,*;q=0.7
Traffic Sample: Apache Killer

HEAD / HTTP/1.1
Host: localhost
Range: bytes=0-,5-0,5-1,5-2,5-3,5-4,5-5,5-6,5-7,5-8,5-9,5-10,5-11,<rybolov deleted this for brevity’s sake>5-1293,5-1294,5-1295,5-1296,5-1297,5-1298,5-1299
Accept-Encoding: gzip
Connection: close
Prepare: Network

- Segmentation of web and other traffic
- “Reasonable” dns ttl (4-8 hours?)
- IDS DDoS rules
  - Counting SYN/IP address
  - Specific layer-5/7 rules
Prepare: Apache mpm_prefork

<IfModule mpm_prefork_module>
  StartServers        8
  MinSpareServers     5
  MaxSpareServers     10
  MaxClients          25
  MaxRequestsPerChild 2000
</IfModule>
Prepare: Caching

- MySQL: Query cache
- Oracle: Query cache
- Content Management System: Content cache
- Content Delivery: Content cache
- Webservers: Static website
Prepare: Site Marketing Metrics

- Browser type
- Operating system
- Country
- Referrer
- Most common URLs
- Publicly-available v/s requires-login
- Average response time
- Average page load time
Prepare: Basic DDoS Mitigation Services

- BGP/scrubbing center
  - All IP traffic
  - Multiple layers of blocking
    - IP
    - TCP
    - Layers 5, 6, 7
- Reverse proxy and CDN
  - Easy to implement (DNS CNAME)
  - Only web traffic
- Cloud hosting and massive scaling

All function better when configured in advance
Detect: Alerts

• External monitoring
• Local server response time
• Network circuit capacity
• Server CPU load
• RAM usage
Detect: Apache mod_status

root@ubuntu:/root# apachectl status
Apache Server Status for localhost
Server Version: Apache/2.2.16 (Debian) PHP/5.3.3-7+squeeze3 with
Suhosin-Patch proxy_html/3.0.1
Server Built: Sep 4 2011 21:02:22

Current Time: Friday, 23-Sep-2011 23:52:25 UTC
Restart Time: Wednesday, 07-Sep-2011 12:36:06 UTC
Parent Server Generation: 3
Server uptime: 16 days 11 hours 16 minutes 19 seconds
Total accesses: 190927 - Total Traffic: 525.0 MB
CPU Usage: u769.16 s35.12 cu0 cs0 - .0565% CPU load
.134 requests/sec - 386 B/second - 2883 B/request
11 requests currently being processed, 6 idle workers
GGR_R____WW..WG.GGG............................................
................................................................
................................................................
................................................................

Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process
Respond: Goals

- Infrastructure stays operational
- Webserver stays operational
- Legitimate users/requests are served
- Other services stay operational
- Limit economic impact
Respond: The “Rough Process”

- Lower DNS TTL
- Flip to provider?
- Initial blocking
- Availability monitoring
- Tune blocking
Block: Traffic Differentiators

- Geography
- IP whitelist or blacklist
- # of requests
- Request timeout
- URL
- HTTP Method
- User-Agent
- Referrer
- Cookie: presence or value
- Logged-in
- CAPTCHA
- WAF rules
The Big WTF?

- No visible traffic signature
- Server processes are “maxed”
- It’s either:
  - Slow DoS
  - Bad code release
- Actions:
  - Block TOR exit nodes
  - Set request timeout to 15-30 seconds
  - Block Russia and Eastern Europe
  - Failover to static site
Giving up: “Scorched Earth Policy”

- Resolve DNS to 127.0.0.1
- Blackhole your ASN
- Failover to maintenance page
- Deny all traffic at ISP
Post-Response

- Post incident review
  - Successes: what worked
  - Failures: what didn’t work
  - Impact: customers, availability, and cost
- Check spam folders for a protection letter
- Logs
- Law enforcement
- Attacker intentions: will they be back?
Thank you!

Securing a Better Internet

© 2010 Akamai