Growing sophistication of DDoS

John Ellis, Enterprise Security Director, Akamai Technologies
The battleground

- 70%
- 50%
- 20Gbps
- 24 hours
- UDP 53 / TCP SSL
- 15x

5
Application attacks
Average for DDoS
Duration of average attack
Achilles' heel
..uses more than attacker
In the beginning ‘he’ made Trin00

July 22nd

February 7

February 8

February 9

Cheap, nasty…and

Note 99-04
do attacked

Yahoo, CNN, eBay

E*Trade, Zdnet

Effective…. ☹️
What’s in a name? Let’s get to the root!

2002 attack against the internet DNS root servers – limited impact


There are 13 Logical DNS root servers – lettered from A to M

The DNS architecture is one of diversity, capacity and any casting technology to provide the foundation of resilience and performance.
You can call me Boris and I have bots baby…

2004
Multibet Australia
Threatened by Russians
Suffered DDoS attack
Paid $25,000
Telco said ....
You can call me Boris and I have bots baby…

if source IP equals Australian IP then accept
Else
deny
Simple C2 architecture back then

- Command & Control Server(S)
- Bot (infected host)
- Target site(S)
- Bot command
- Attacker
First the script kiddie, now the bot-kiddie
Source of attack traffic – as seen by Akamai

SECURITY: ATTACK TRAFFIC

Nearly 51% of observed attack traffic originated in the Asia Pacific/Oceania region, while just over 23% originated in North and South America and just under 25% originated in Europe. The remaining 1% of attack traffic originated in Africa.

33%  China
13%  United States
4.7%  Russia
4.5%  Taiwan
4.3%  Turkey
3.8%  Brazil
2.7%  Romania
2.5%  India
1.7%  Italy
1.5%  South Korea
28%  Other

*The blue areas represent each country’s percentage of the overall total amount of attack traffic observed by Akamai.*
Operation Ababil – Financial Service DDoS

- 18 September 2012 ‘Cyber fighters of Izz ad-in Al qassam’ called on hacktvists to join-in a cyber campaign against American FSI

- Multistage campaign attacking a number of major FSIs such as NYSE, BoA, JPMC

- Akamai saw attack traffic in excess 65Gbps

- Initial campaign lasted for five days in which all targets experienced significant service disruption
Some interesting observations (the technical stuff)

- Used compromised VPS/Cloud Server 'Google hacking'
- Use of DDoS toolkit "itsoknowproblembro"
- Booter Scripts: indx.php, stcp.php, stph.php
- Traffic per node of ~100Mbps
- 700-1500 attacking nodes
- Simplified/quick C2
- Quick node recruitment/replacement

In a word ‘Nasty’
‘itsoknoproblembro’ C2 architecture
‘itsoknoproblembro’ C2 architecture

Command & Control Server(S)  Bot (infected host)  Target site(S)

Bot command

Attacker
US bank attacked at 12:44 PM 03 January 2013

- Gomez benchmark of bank home page, measured from 12 cities 1x per hour.
- First outage recorded at 12:44 PM.
- Attack continued to 6:21 PM.
Traditional mindset in dealing with DDoS

Deploy significant capacity in the data center ……to absorb ‘flash’ crowds and peaks in high traffic loads

Leverage network security defenses like firewalls, intrusion prevention systems, and load balancers………to inspect, filter, and manage network traffic

Engage with Internet service provider for……… a ‘clean’ pipe service or ‘scrubbing’ service
But we built this city on firewalls

Network Firewall: 27%
IPS: 24%
Load Balancer: 8%
Application: 30%
Database: 5%
What happened? Why did so many banks struggle?

Deploy significant capacity in the data center to absorb 'flash' crowds and peaks in high traffic loads.

Engage with Internet service providers for a 'clean' pipe service or 'scrubbing' service.

Clean pipe solutions offer limited protection. Still places significant strain of perimeter defenses.

Increased cost, addresses less than 40% of DDoS attacks.

Leverage network security defenses like firewalls, intrusion prevention systems, and load balancers to inspect, filter, and manage network traffic.

Often targets of the attacks and have limited capacity to deal with scalable attacks.
Observations, and things to ponder

How must our security protections evolve to get and stay ahead of the rapid changes?

How can we be more resilient to attacks, whilst containing costs?

My online platforms need to perform irrespective if they are under attack.

Solutions need to deliver real-time protection, and not wait for ‘people’ to determine what to do next.
Do we need K to deploy the arcnet?

- Poor Performance & Availability
- Attackers hit origin infrastructure directly, stressing shared resources

Without arcnet…..
Do we need K to deploy the arcnet?

With an inline cloud solution
- Origin is “cloaked”
- Attackers are blocked in the cloud, AWAY from the origin infrastructure

Result
- Sustained Performance & Availability
Protect ALL Layers of the OSI stack

Multi-Layered Defense

- **Layer 1 (Physical Connectivity)**
  - Physical Connectivity

- **Layer 2 (Local Network Connectivity)**
  - Local Network Connectivity

- **Layer 3 (ICMP Flood)**
  - ICMP Flood

- **Layer 4 (TCP SYN Flood)**
  - TCP SYN Flood; Attack against non-web ports (non-80/443)

- **Layer 5-7 (Flood of requests for cached objects)**
  - Flood of requests for cached objects
  - Requests for non-cacheable content; XSS; SQL-injection, etc

- **Layer 6-7 (WAF)**
  - WAF blocks application-layer attacks

- **Layer 5-7 (non-cacheable)**
  - Absorbs/blocks ALL attacks against cacheable content

- **Layer 1-4 (WAF)**
  - Blocks ALL attacks against layers 1 through 4

Dramatically Reduced Possible Attack Surface

Customer Origin
A bank that used a Cloud ‘arcnet’ solution *Always on Protection*

- Top financial services firm with nearly 10M customers.
- Peak attack traffic was 30 Gbps, 30x normal daily high traffic.
- Attackers gave up after 15 minutes, and moved attack to another bank.
- 100% of the attack was on SSL.

![Graph showing peak traffic](image-url)
Massive Banking DDoS Attack

- Akamai offloaded 100% of the attack.

```
<table>
<thead>
<tr>
<th>TOTAL VOLUME</th>
<th>% VOLUME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Responses</td>
<td>1.9 TB</td>
</tr>
<tr>
<td>Midgress Responses</td>
<td>3.5 GB</td>
</tr>
<tr>
<td>Requests</td>
<td>48 GB</td>
</tr>
<tr>
<td>Origin Responses</td>
<td>348.9 MB</td>
</tr>
</tbody>
</table>
```

- "A bug impacting our windshield".

(Attack ended at 11:25)
And Perform….you must

• Gomez banking benchmark for this site. 12 U.S. measurement agents.

• No performance impact during this attack. 100% availability. No outliers.
Before we say goodbye….

….what alternative is there to the internet?

Innovation is vital to capitalizing the opportunities

The internet has inherit issues with performance and security

You can make the internet work for you…..

….protect your investment, succeed even when under attack

….move closer to your users and the attackers, accelerate the good, block the bad