DDoS Attacks - Peeling the Onion on One of the Most Sophisticated Ever Seen

Eldad Chai, VP Product
Incapsula – Application Delivery from the Cloud

Application aware CDN

- Website/App Security
- Acceleration
- DDos Protection
- Load Balancing & Failover
• **Volume Based Attacks**
  > **Method**: Include UDP floods, ICMP floods, and other spoofed packet floods.
  > **Objective**: Saturate the bandwidth of the attacked site.
  > **Magnitude**: Typically measured in Bits per second.
DDoS 101

- **Protocol Attacks:**
  > **Method:** Primarily SYN floods, but also fragmented packet attacks.
  > **Objective:** Consume web server resources or intermediate communication equipment, such as firewalls and load balancers.
  > **Magnitude:** These are usually measured in Packets per second.
• Application Layer Attacks

  > **Method:** Unlike protocol attacks, these are comprised of legitimate and seemingly innocent requests.
  > **Objective:** Bring the application servers down.
  > **Magnitude:** Requests per second.
Where do we stand today?

Attacks bandwidth is showing exponential growth

Two thirds of attacks exceed 10Gbps
More than 13% exceed 40Gbps
It’s not all bandwidth

More than 25% of attacks exceed 10Mpps
Most IPS/IDS will crash at 5Mpps
Recent campaigns / SaaS applications

**Meetup**

We’re standing up against a DDoS attack

No doubt, this has been a tough weekend for Meetup. Since Thursday, we faced a massive attack on our servers – a DDoS attack, which is a barrage of traffic intended to make service unavailable. We’ve had

**Basecamp**

Basecamp was under network attack this morning

David wrote this on Mar 24 / 12 comments

Criminals attacked the Basecamp network with a distributed denial-of-service attack (DDoS) this morning. The attackers tried to extort us for money to make it stop. We refused to give in and worked with our network.

**Bitly**

We are currently working to mitigate a DDoS attack. Some of our site may be unavailable, but we’re working to restore full functionality.

Follow

@Bitly

Reply Retweet Favorite More

**Vimeo**

Vimeo January 16, 2013 - 0

We apologize for this inconvenience.

We're dealing with a DDoS attack that's been causing instability all day. Right now, embedded videos are up and running, but vimeo.com is only accessible to about half of our users. We understand your frustration and truly apologize for it. Vimeo is a big website and attacks happen, but this is by far the most aggressive we've seen in 7 years. Please be advised that we're doing all that we can to resolve these issues as quickly as possible.

Thanks again for your patience.
How are attackers reaching these numbers?

• Are botnets becoming bigger?
  > No, according to www.shadowserver.org

• Are there more open DNS resolvers?
  > No, the number is actually declining according to www.openresolverproject.org

• Are there more open NTP servers?
  > Probably not, www.openntpproject.org

• So what is it then?
How are attackers reaching these numbers?

- They are using bigger guns

<table>
<thead>
<tr>
<th>IP</th>
<th>Pps</th>
<th>Kbps</th>
<th>Suspicious</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1,281,612 pps</td>
<td>768,968 Kbps</td>
<td>1,281,612 pps</td>
</tr>
<tr>
<td>2</td>
<td>933,892 pps</td>
<td>560,336 Kbps</td>
<td>933,892 pps</td>
</tr>
<tr>
<td>3</td>
<td>544,756 pps</td>
<td>326,854 Kbps</td>
<td>544,756 pps</td>
</tr>
<tr>
<td>4</td>
<td>503,324 pps</td>
<td>301,995 Kbps</td>
<td>503,324 pps</td>
</tr>
<tr>
<td>5</td>
<td>375,568 pps</td>
<td>225,341 Kbps</td>
<td>375,568 pps</td>
</tr>
<tr>
<td>6</td>
<td>302,196 pps</td>
<td>181,318 Kbps</td>
<td>302,196 pps</td>
</tr>
<tr>
<td>7</td>
<td>176,896 pps</td>
<td>106,138 Kbps</td>
<td>176,896 pps</td>
</tr>
<tr>
<td>8</td>
<td>166,416 pps</td>
<td>99,850 Kbps</td>
<td>166,416 pps</td>
</tr>
<tr>
<td>9</td>
<td>146,672 pps</td>
<td>88,004 Kbps</td>
<td>146,672 pps</td>
</tr>
<tr>
<td>10</td>
<td>130,148 pps</td>
<td>78,089 Kbps</td>
<td>130,148 pps</td>
</tr>
</tbody>
</table>

Example of a 4Mpps attack
Less than 30 IPs are generating more than 99% of the traffic
Peeling the Onion on One of the Most Sophisticated Attacks Ever Seen
The players

- Polish hackers

VS

- Successful SaaS Platform
- Very competitive online trading industry
Round 1
Round 1 - Volumetric Attack

• 30Gbps SYN Flood
• Typical of any DDoS attack
  > Easy to perform (Given the resources)
• No amplification was used
Round 1 – Win, Geo distribution

- Geo Distribution of attack traffic (sharing the load)
- Dedicated networking capabilities to deal with volumetric attacks
- Aggressive blacklisting of offending IP addresses
Round 2
Round 2 – HTTP Flood

- Layer 7 - 100K Req/Sec
- Targeting “resource intensive” pages
- “The smoke screen”
  - This type & level of attack persisted for weeks
Round 2 – Win, spot the bot

• Anti bot technology

• Non intrusive differentiation between legitimate browsers and bots

• Good bots vs. Bad bots
  > Google / Bing / Yandex / Baido = Good
  > DDoS agents = Bad
Round 3

INTERNET EXPLORER POPUPS
It's a trap!
Round 3 – Real browsers on call

- Legit traffic?
Round 3 – Real browsers on call

I want to know, why Internet Explorer opens 20 windows with your product without my permission. This is so upset and I want to know why you do this and how can I avoid that pages?
Round 3 – Win, Pushdo CAPTCHA

We got one! It’s Pushdo

O look, it’s calling home

```
GET /9D7D4F88/C124DE0.dat HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; YPC 3.2.0; CLR 2.0.50727; Media Center PC 5.0; InfoPath.2; .NET CLR 3.5.30729; .NET Host: Cache-Control: no-cache
HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: G?MT
Content-Type: application/octet-stream
Content-Length: 128
Last-Modified: GMT
Connection: keep-alive
ETag: “51f7d6ea-80”
Accept-Ranges: bytes

...X.A.....Ad.p+...1.f!5...#8.Tdf.'....'Nw...3S.G.U.
4p.q6.@4P4........07[q]k..xx.j..e.[]........
p.bv]```

Botnet CnC

Encrypted Payload
Round 4

The Phantom's Revenge
Round 4 – Headless Browsers

- Headless browsers leveraging Phantom JS were being used to emulate real users
  - Generating 700 Million requests / Day
Round 4 – Win, Phantom JS fingerprinting

• Reverse engineering Phantom JS Kit
• Crafting a signature to identify all bots using the kit
• Yes, CAPTCHA solving Firefox!
Round 5 – Win, Javascript injection to the rescue

• Added some JavaScript to the CAPTCHA page template

• The JavaScript logs the user typing the CAPTCHA challenge

• A-Ha! The attackers are not typing the CAPTCHA
Round 5 – Adaptation

• A week later, attackers are typing CAPTCHA 😞
Round 5 – Win, Javascript injection to the rescue

• HEHE! Typing Slow 😊

• Seems it takes them more than a minute to start typing the CAPTCHA

• Added a JS that puts a time limit on the CAPTCHA
Round 5 – Adaptation

- The clients that manage to be quick still cause damage
- Randomizing URLs
Round 5 – How we won

• Tracking DDoS botnets – Same botnet is used to launch the Firefox attacks

• ~200K unique IP per day
The aftermath

• DDoS can resemble APTs
• Visibility is crucial
• Analyzing different levels of the interaction is crucial
• Reacting fast is crucial
Thank you
Please send follow up questions to eldad@incapsula.com