Preparing for the Imminent Terabit DDoS Attack

Orion Cassetto, Sr. Product Marketing Manager, Incapsula
Agenda

- Network DDoS trends
- Is a Terabit DDoS attack imminent?
- Attributes of a DDoS-resilient network
- Infrastructure and DNS protection
Incapsula, An Imperva Company

- Founded in 2009 by a group of security industry veterans with strong expertise in web application security, online safety, and identity theft
- Spun out of, and subsequently, acquired by Imperva
- Cloud-based solution includes
  - Enterprise-grade Website Security
    - PCI-certified Web Application Firewall
  - DDoS Protection
  - Load Balancing & Failover
- All fully integrated on top of our global CDN
Orion Cassetto  
Sr. Product Marketing Manager, Incapsula  

- Product Marketing Manager for Incapsula  
- Previously held product marketing positions at Imperva and Armorize Technologies  
- Experienced in Web app security and SaaS security solutions  
- Holds degrees in Asian Studies and Chinese Language from Washington State University
DDoS Landscape – Attacks Getting Bigger

In 2013 we saw a gradual increase in peak attack volumes

Today, we see this trend continuing. 2014 already presented us with several ~100Gbps threats, including a 180Gbps NTP DDOS attack.
Average DDoS Attack Sizes Are Growing

Not only are big attacks getting bigger, average attack sizes are also growing – in 2013 the mean attack size was 10Gbps.

Source: 2014 Verizon Data Breach Investigation Report
Where Do We Stand Today?

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

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 was under network attack this morning

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

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

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.
Recent Campaigns / DNS Providers

**UltraDNS**

Victor Trac
@victortrac

Neustar/@UltraDNS has had a system wide outage this morning without a single public ack & no status page. Interesting way to run a company.

**Point DNS**

Point DNS
@pointdns

We're experiencing a DDoS attack on all DNS servers we are working hard to mitigate the attack.
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>550,336 Kbps</td>
<td>933,892 pps</td>
</tr>
<tr>
<td>3</td>
<td>544,756 pps</td>
<td>325,854 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>105,138 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>79,089 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
What Can We Learn From All This?

- The stronger the Internet becomes, the stronger the attacks
- The largest attacks use a small set of super resources rather than a large set of weak resources
- Attacks will far exceed a single network’s capacity
- Can we expect a 1Tbps+ attack within the next 12-36 months?
A DDoS Resilient Network

Scalable architecture
Scalable business model
= Cloud

Different assets need different protection
(FTP != HTTP != DNS)

Capacity scale
In depth protection

Rapid response
Visibility

React quickly to preserve the false positive to false negative balance

You can’t defend yourself from what you don’t see
Threats Facing Various Online Services

- **Application data**
- **TCP / UDP**
- **SSH**
- **FTP**
- **DNS**
- **HTTP**

**Advanced persistent threats (APT)**
- SQL injection

**DNS query attack**
- POST flood

**SYN flood**
- DNS amplification
- NTP amplification
- Direct IP attacks
Incapsula DDoS Protection

Application data

Incapsula Web Application Firewall

Incapsula Application protection
Incapsula DNS protection

Incapsula Infrastructure protection
Incapsula Application Protection

Always On / On Demand

HTTP/S Requests
From Cache

HTTP/S Proxy

Only Safe HTTP/S Requests
Web servers [HTTP/S]

Protect HTTP/S Applications

Layer 3&4 and also Layer 7

Legitimate Users

HTTP/DOS Traffic
Incapsula DNS Protection - NEW

Always On Service

- Protect DNS servers
- Prevent Blacklisting
Incapsula Infrastructure Protection - NEW

On Demand Service

Customer's IP Range

Protect all services and protocols

Protect entire IP ranges

Legitimate Users

Layer 3&4 (Network)

BGP ANNOUNCEMENT

GRE Tunnel
(Clean Pipe)

DDOS Traffic

Customer's DMZ
Scaling BGP

IP ranges are announced in Anycast

23.5.6.0/24

LAX 80 Gbps

23.5.6.0/24

IAD 60Gbps

23.5.6.0/24

FRA 80Gbps

Customer’s DMZ
Imperva Positioned as a Magic Quadrant Leader


This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Imperva. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.
Webinar Materials

Join Imperva LinkedIn Group, Imperva Data Security Direct, for…

- Post-Webinar Discussions
- Answers to Attendee Questions
- Webinar Recording Link
- Join Group
Questions?

www.imperva.com
Thank You