

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



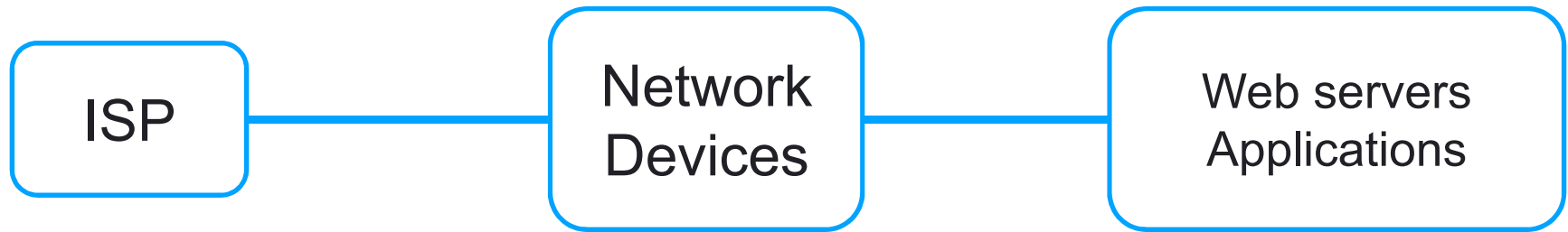
DDos
Protection

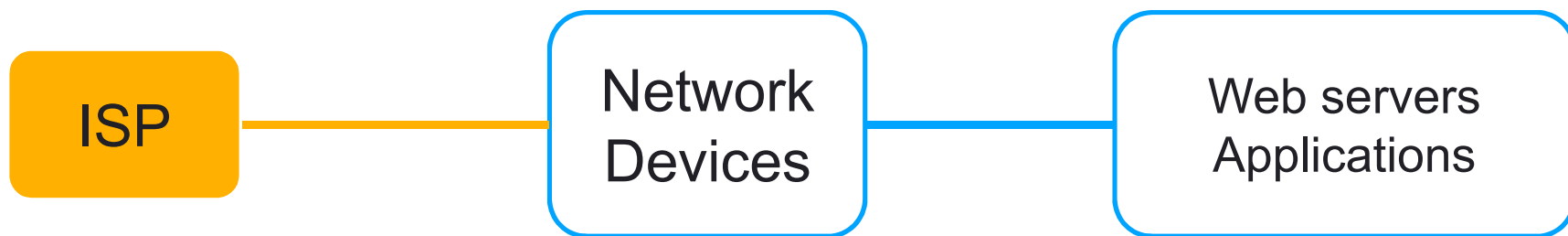


Load Balancing
& Failover



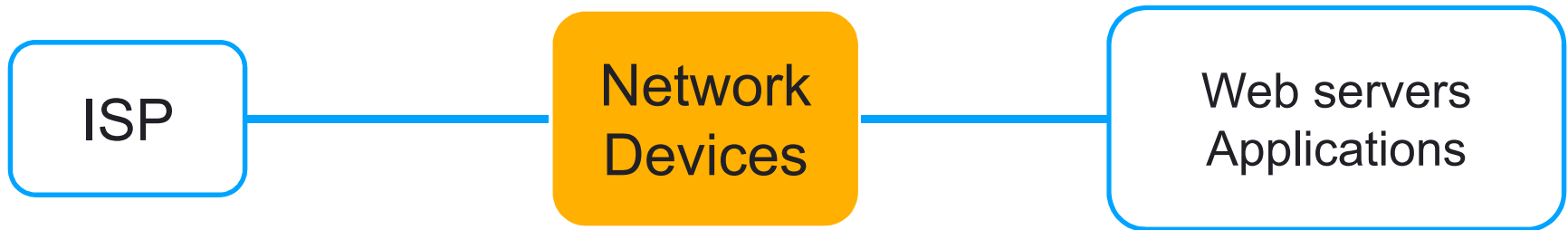
DDoS 101





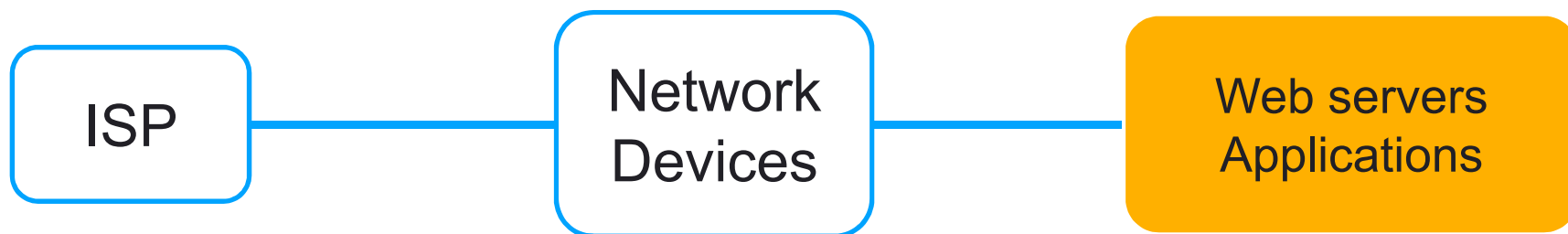
- **Volume Based Attacks**

- > **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.



- **Protocol Attacks:**

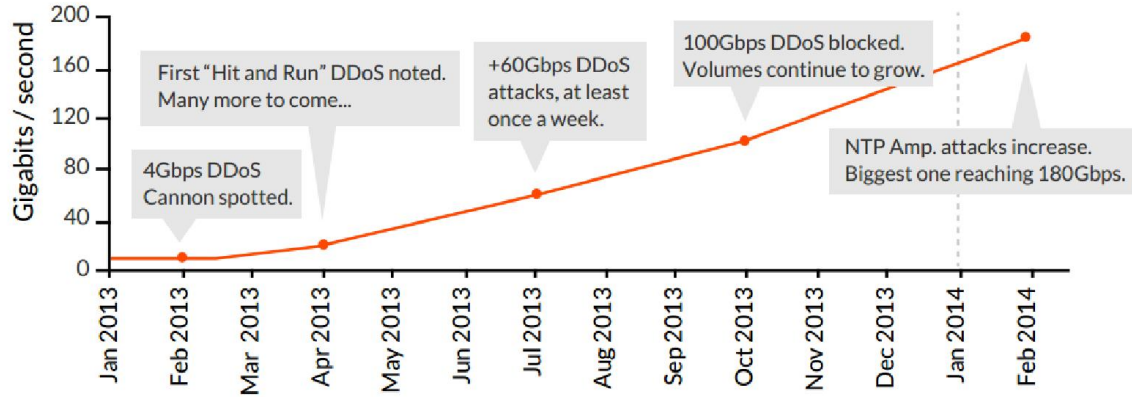
- > **Method:** Primarily SYN floods, but also fragmented packet attacks.
- > **Objective:** Consume web server resources or intermediate communication equipment, such as firewalls and load balancers.
- > **Magnitude :**These are usually measured in Packets per second.



- **Application Layer Attacks**

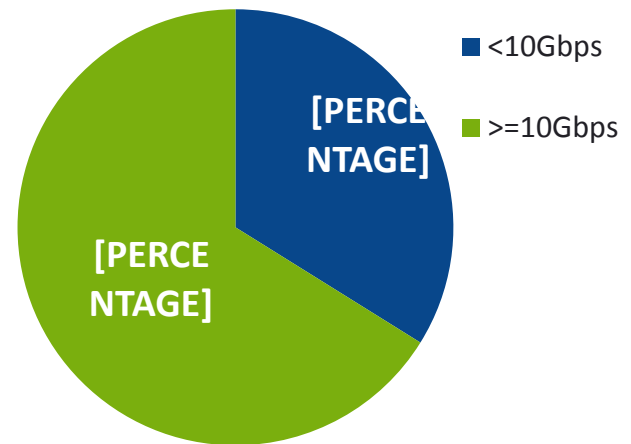
- > **Method:** Unlike protocol attacks, these are comprised of legitimate and seemingly innocent requests.
- > **Objective:** Bring the application servers down.
- > **Magnitude:** Requests per second.

Where do we stand today?

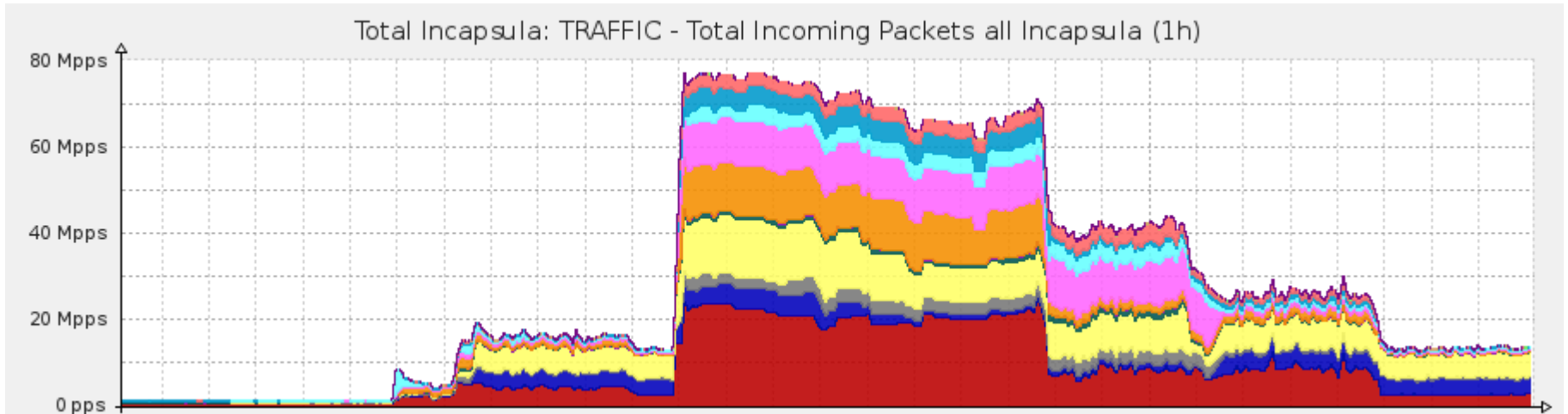


Attacks bandwidth is showing exponential growth

**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



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
@Bitly

Follow

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

Reply Retweet Favorite More



Vimeo

January 16, 2013 ·

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.

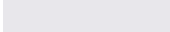
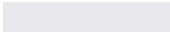
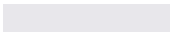
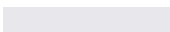
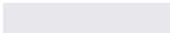
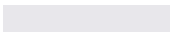
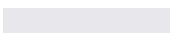
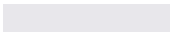
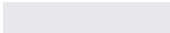
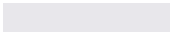
Thanks again for your patience.

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

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

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



VS



- Polish hackers

- Successful SaaS Platform
- Very competitive online trading industry

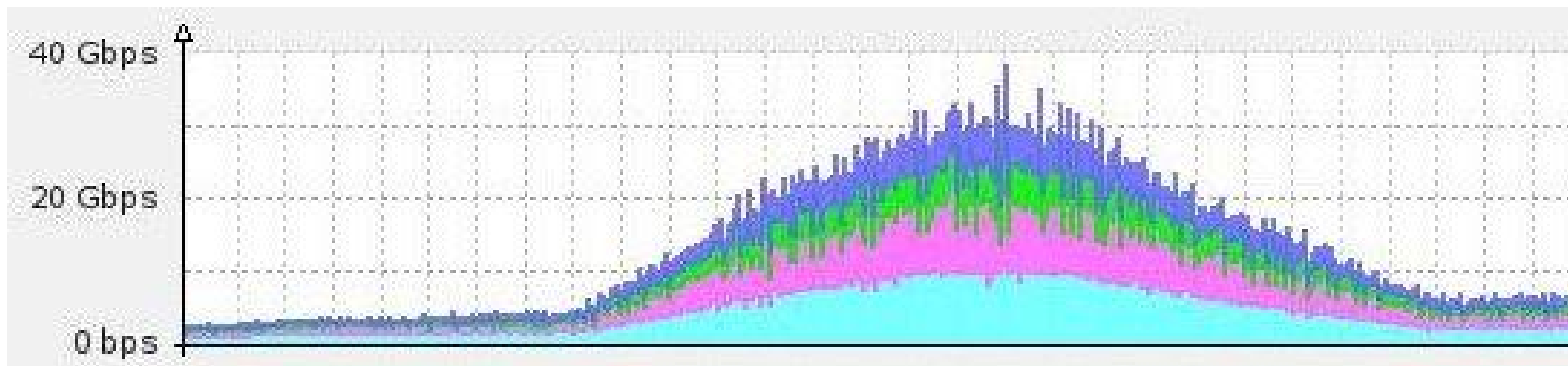
 Incapsula

Round 1



Round 1 - Volumetric Attack

- **30Gbps SYN Flood**
- **Typical of any DDoS attack**
 - > **Easy to perform (Given the resources)**
- **No amplification was used**

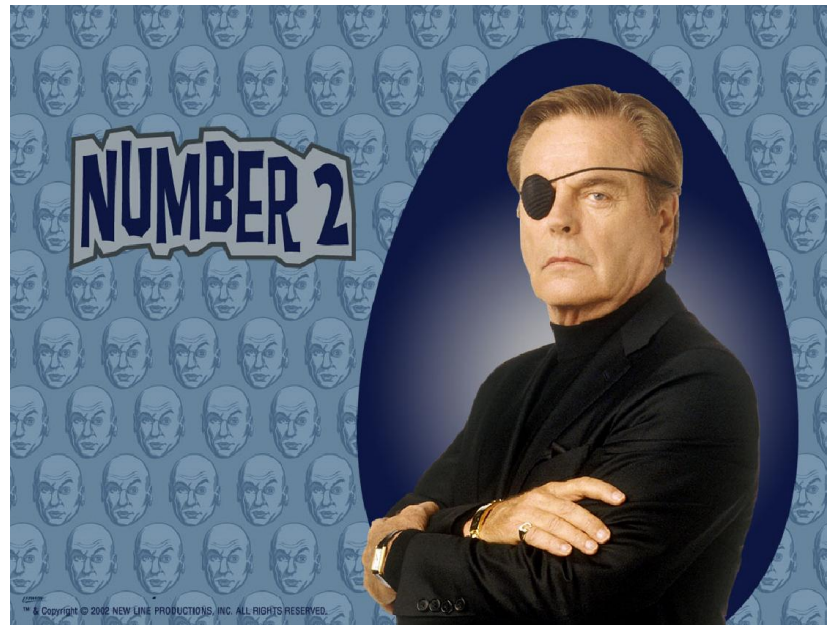


Round 1 – Win, Geo distribution

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

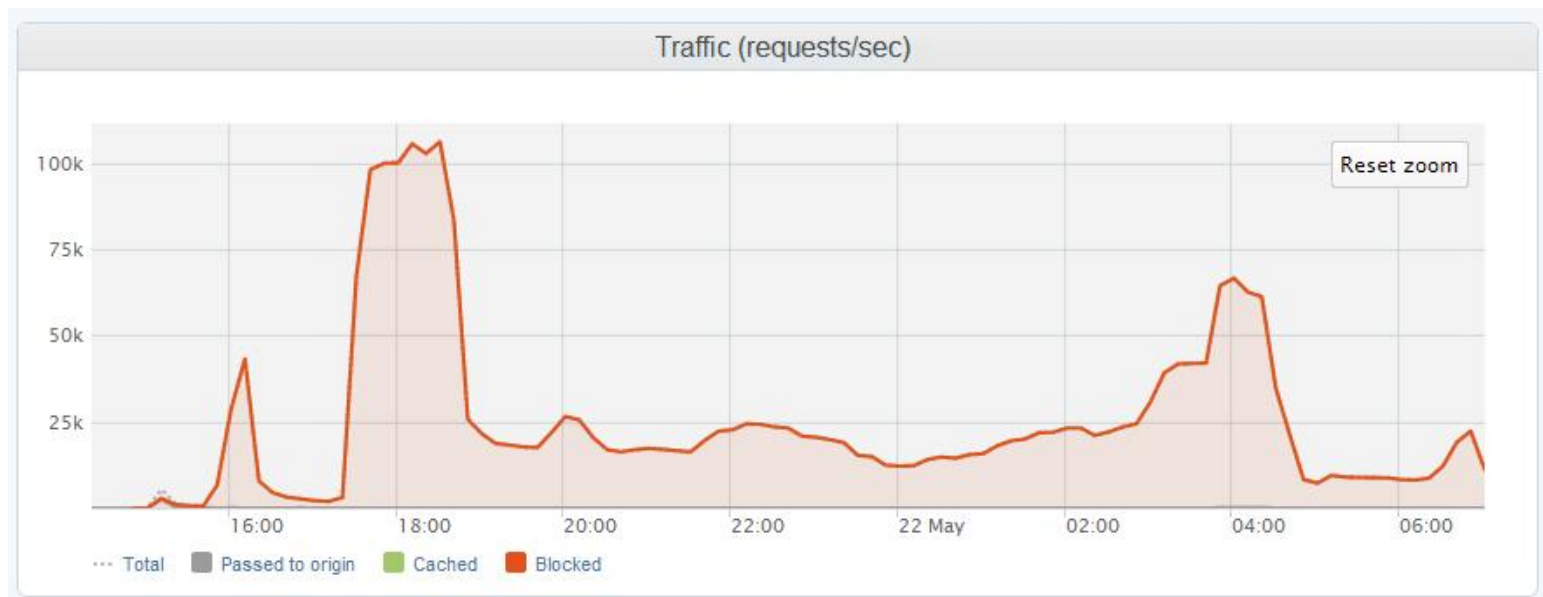


Round 2



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

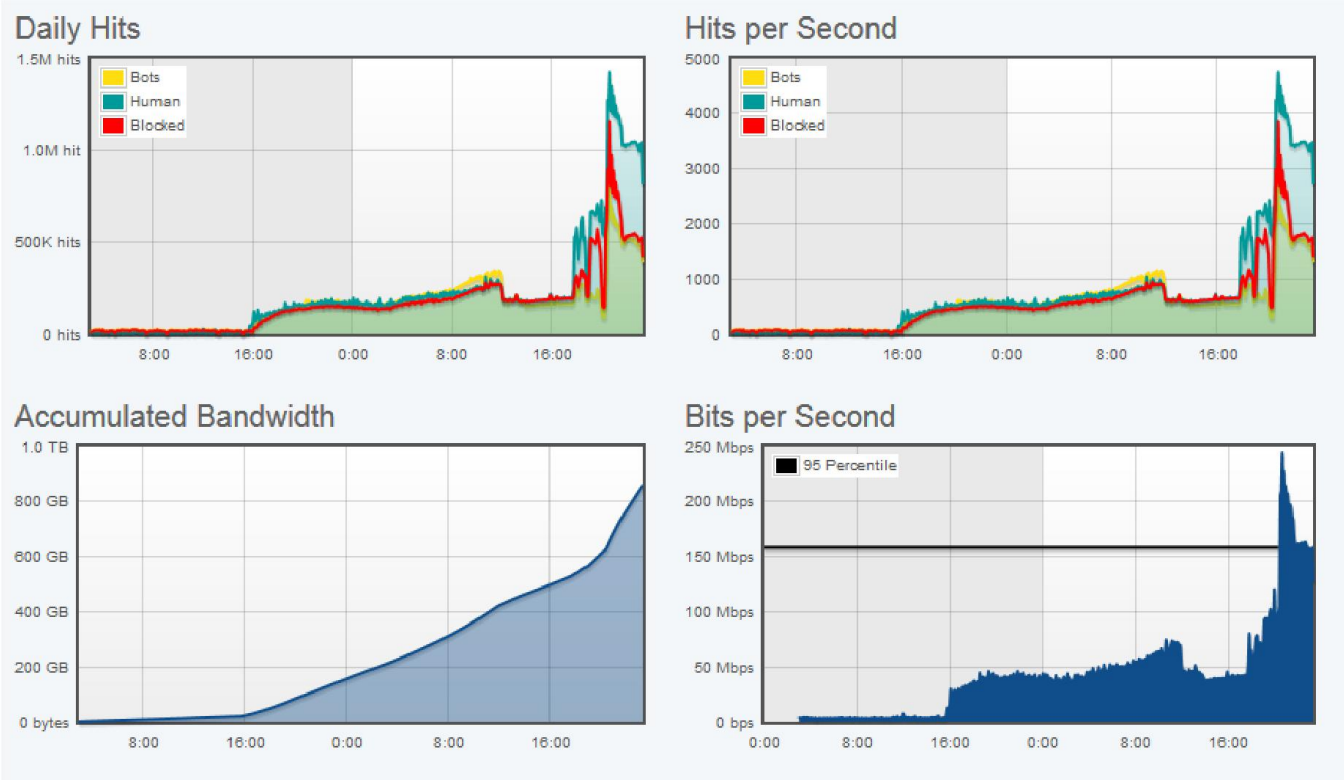


Round 3



Round 3 – Real browsers on call

- Legit traffic?



Round 3 – Real browsers on call



Blurred text, likely a name or email address, positioned above the main text.

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 /9d7d4fbb/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: ██████████ ← Botnet CnC
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx/1.4.1
Date: ██████████ GMT
Content-Type: application/octet-stream
Content-Length: 128
Last-Modified: ██████████ GMT
Connection: keep-alive
ETag: "51f7d6ea-80" ← Encrypted Payload
Accept-Ranges: bytes

.....X.A.. ^D.p...+. .1.f!5...:#,8...TdF.'.....'NW. ..3S.G..U.
+lp...q6..@P4.....07{qjk...xx.j.....e.{}.....,
p..bvX
```

Image Name	PID	User Name	CPU	Mem Usage
wuauclt.exe	3028		00	656 K
wscntfy.exe	1336		00	200 K
wmiprvse.exe	4292	NETWORK SERVICE	00	1,576 K
werehost.exe	2792		00	6,832 K
winlogon.exe	540	SYSTEM	00	1,332 K
VBoxTray.exe	1916		00	352 K
VBoxService.exe	820	SYSTEM	00	932 K
taskmgr.exe	2508		00	2,896 K
System Idle Process	0	SYSTEM	00	28 K
System	4	SYSTEM	01	52 K
svchost.exe	2192		01	29,176 K
svchost.exe	1992		00	29,168 K
svchost.exe	1988		00	29,016 K
svchost.exe	1136	LOCAL SERVICE	03	1,332 K
svchost.exe	1092	NETWORK SERVICE	00	1,344 K
svchost.exe	1044	SYSTEM	00	10,968 K
svchost.exe	1000		00	29,840 K
svchost.exe	952	NETWORK SERVICE	00	1,928 K
svchost.exe	864	SYSTEM	00	1,336 K
svchost.exe	508		00	948 K
svchost.exe	220	LOCAL SERVICE	00	80 K
spoolsv.exe	1472	SYSTEM	00	104 K
smss.exe	368	SYSTEM	00	56 K
services.exe	652	SYSTEM	00	1,640 K
msmmsg.exe	1932	SYSTEM	00	272 K
lsass.exe	664	SYSTEM	00	2,196 K
inetinfo.exe	5944	SYSTEM	00	9,936 K
explorer.exe	6588		07	65,144 K
explorer.exe	6012		60	69,012 K
explorer.exe	5988		11	70,888 K
explorer.exe	5940		00	14,612 K
explorer.exe	5904		13	71,752 K
explorer.exe	4356		00	14,672 K
explorer.exe	4216		02	72,948 K
explorer.exe	4072		00	14,632 K
explorer.exe	3824		00	14,620 K
explorer.exe	3820		00	14,648 K
FortSISSLVNdsem...	276	SYSTEM	00	64 K
explorer.exe	1616		00	5,172 K
ctfmon.exe	1924		00	840 K
csrss.exe	516	SYSTEM	01	1,964 K
cmd.exe	2652		00	116 K
alg.exe	444	LOCAL SERVICE	00	200 K

Round 4



Round 4 – Headless Browsers



- Headless browsers leveraging Phantom JS were being used to emulate real users
 - > Generating 700 Million requests / Day

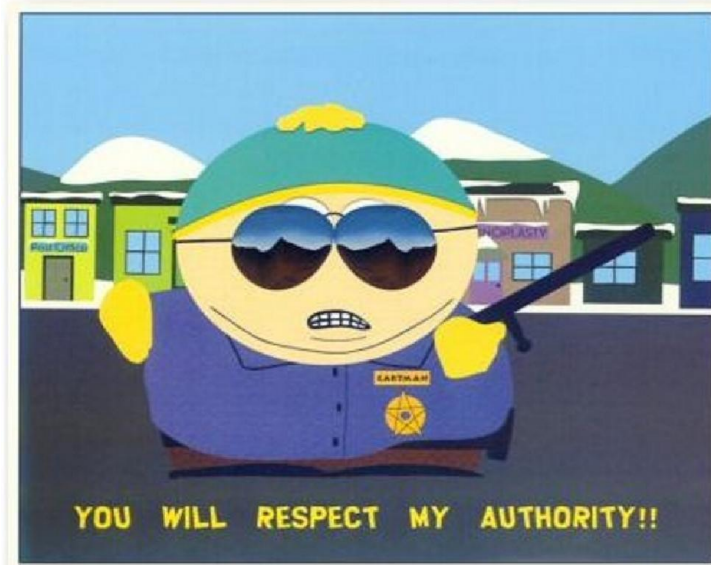


Round 4 – Win, Phantom JS fingerprinting

- Reverse engineering Phantom JS Kit
- Crafting a signature to identify all bots using the kit

The screenshot displays a bot detection interface. On the left, a red-bordered box contains the text "PhantomJS (Developer Tool) from Mexico". To the right, a summary of bot activity is shown: "189.155.92.122 | 2 page views | 2 hits | Supports Cookies". Below this, several fields are listed: "Entry Page:" (blurred), "User Agent: Mozilla/5.0 (Windows NT 6.2 rv:18.0) Gecko/20100101 Firefox/18.0", "Served Via: San Jose, CA", and "Session Id: 124000470067772402". A "Threat @" field shows a list of links: "email", "raw", "syslog", "Internal", "syslog", and "API". Below this, a "Raw:" field shows a link to "raw visit". Two red arrows point from the "Threat @" field to the "raw visit" link. At the bottom, two orange buttons indicate "1 DDoS" and "CAPTCHA (Fail)". On the right side, there are "Actions" and "More" dropdown menus.

Round 5



Round 5 – CAPTCHA solving Firefox???

57 minutes ago	Firefox from Bolivia	190.129.19.43 First Visit: 3 months ago 10 page views 57 hits Supports Cookies Supports JavaScript Entry Page: [REDACTED] User Agent: Mozilla/4.0 (compatible MSIE 6.0 Windows NT 5.1 SV1) Served Via: Miami, FL Session Id: 169000340116687488 CAPTCHA (Pass)	Actions Less
URL: [REDACTED] (GET)		Status: Client was sent a CAPTCHA security check, request was suspended	
DDoS (Request suspended)		Add to whitelist	
		CAPTCHA DDoS	
URL: [REDACTED].gif (GET)		Response code: 200 Response time: 0ms	

- 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