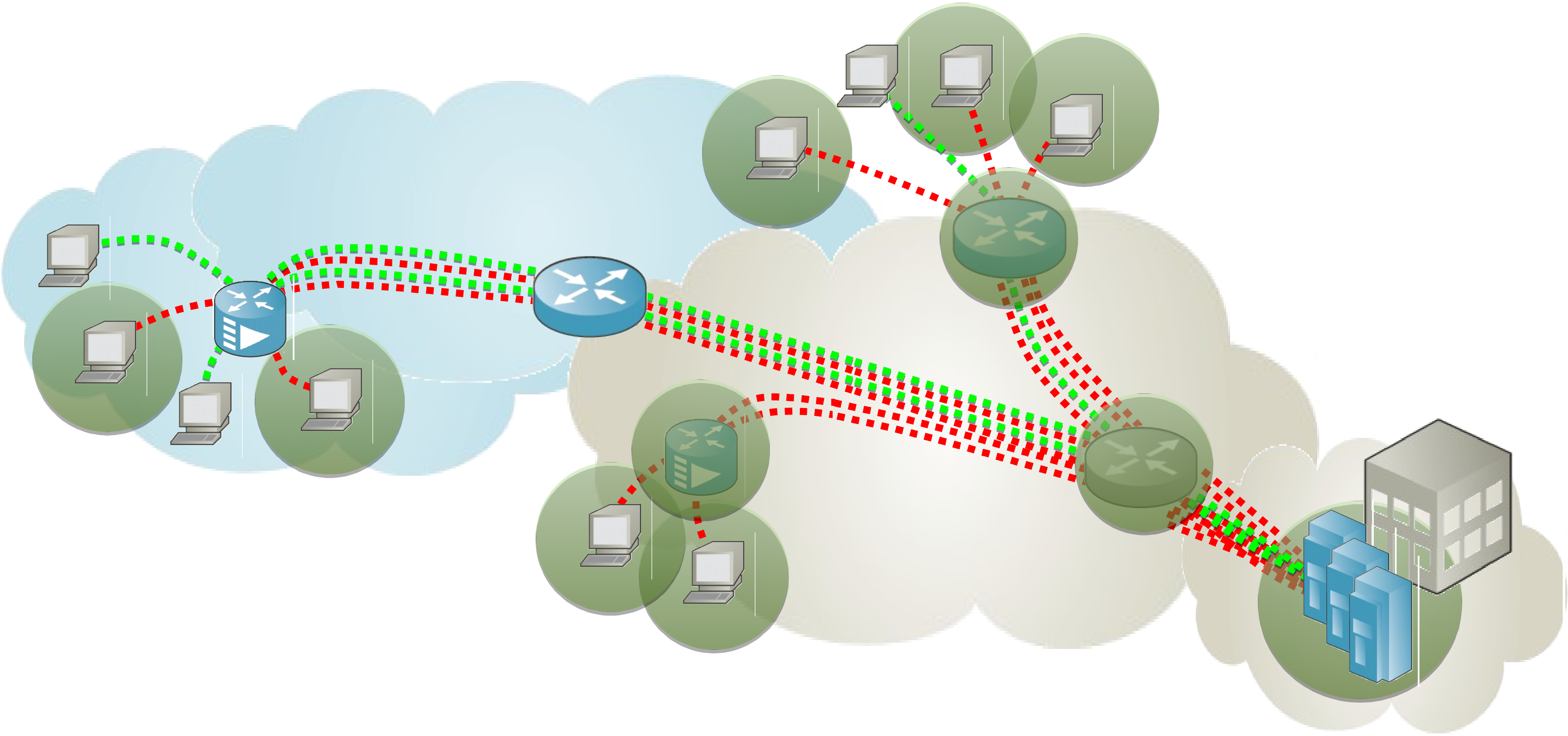
ARBOR NETWORKS
The Security Division of NETSCOUT

# Understanding the New Threat Landscape with the Global Threat Intelligence

# DDOS ( DISTRIBUTED DENIAL OF SERVICE ) ATTACK



A **Distributed Denial of Service (DDoS) attack** uses compromised hosts or bots from distributed sources to overwhelm the target with illegitimate traffic, preventing servers from responding to legitimate requests.

# WHO IS ARBOR NETWORKS ?

**107 countries**
Where Arbor Networks solutions are deployed

**16 years**
Delivering security and network visibility innovation

**Global traffic visibility**
Hundreds of terabits of global Internet traffic intelligence

90%+ of the world's
**Tier 1 service providers**

8 of the 10 largest
**Cloud service providers**

9 of the 10 Largest
**Managed security service providers**

**55% of revenue**
From Global Customers in Asia, Europe and Latin America.

**#1 provider**
DDoS mitigation to Carrier, Enterprise and Mobile, IHS Infonetics, June 2015

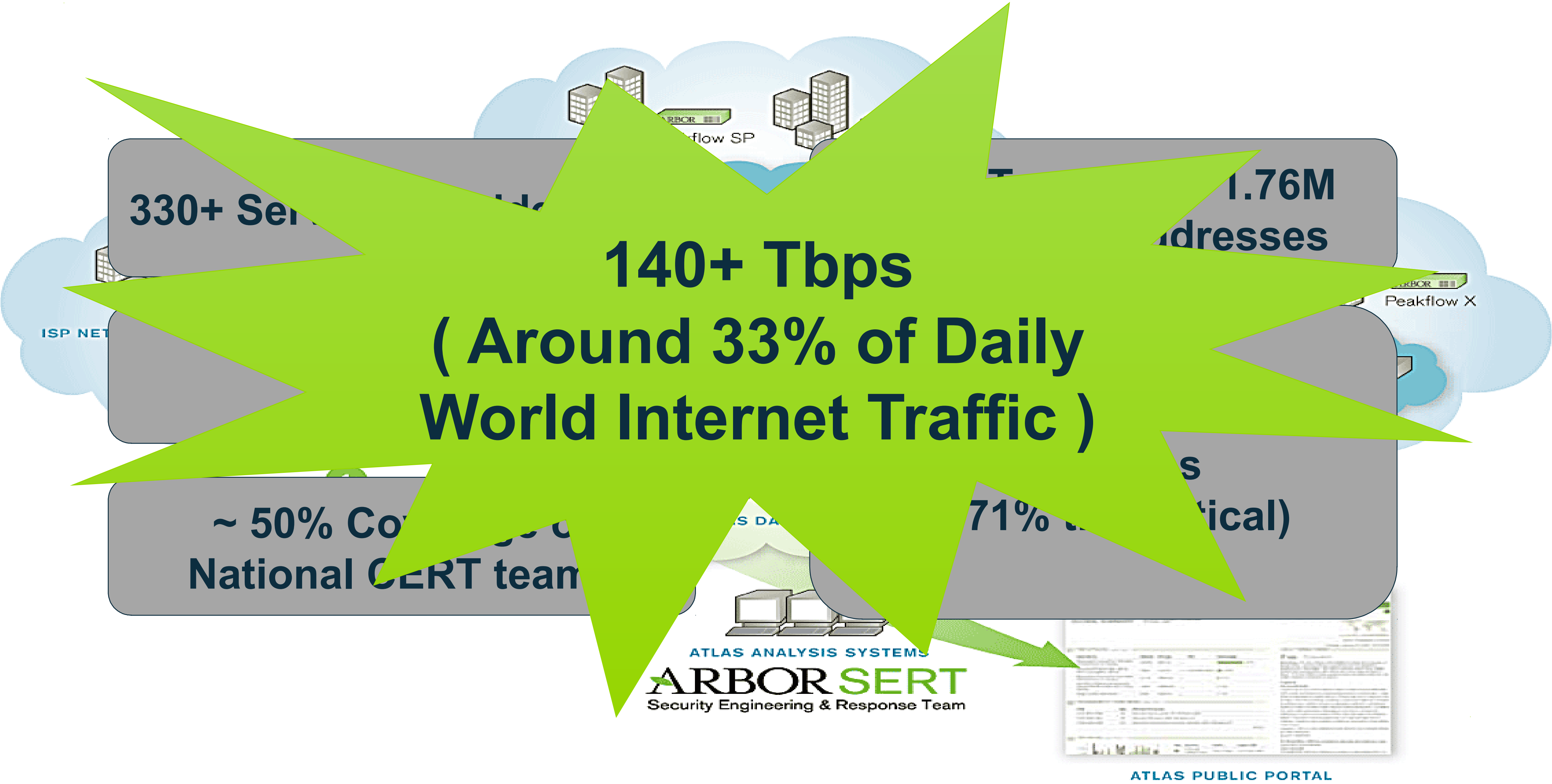
**5 Olympic games**
Protected by Arbor Networks

3 of the 5 Largest
**Social media networks**

5 of the 6 Largest
**U.S. cable broadband providers**

4 of the Top 6
**U.S. banks based on assets under management**

# Arbor Security Engineering Respond Team (ASERT) : ATLAS Sensors



330+ Se ide

T 1.76M
ddresses

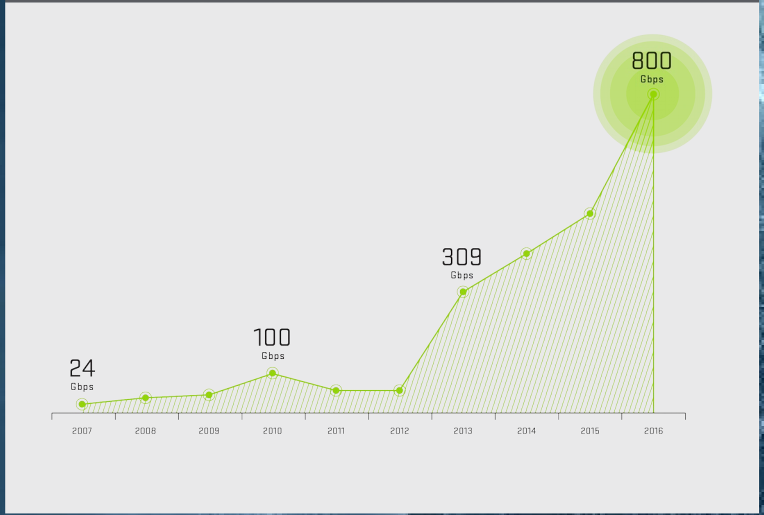
s
71% t tical)

~ 50% Co ge o
National CERT team

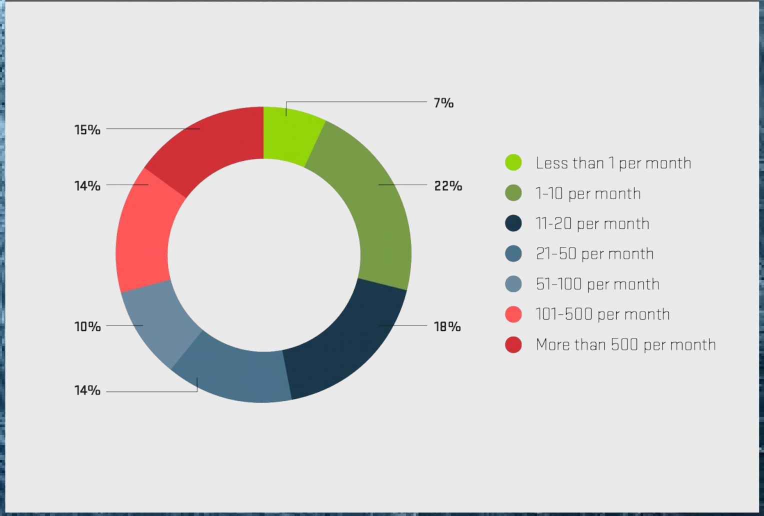
140+ Tbps
( Around 33% of Daily
World Internet Traffic )

# The Stakes Have Changed

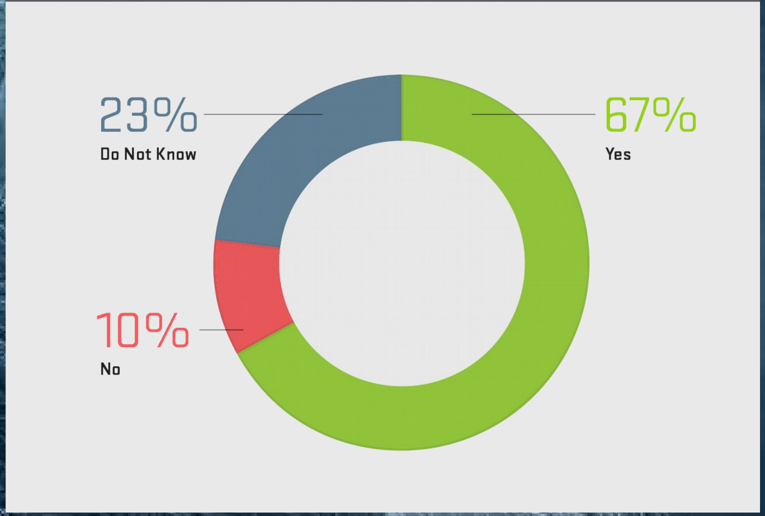
## SIZE



## FREQUENCY

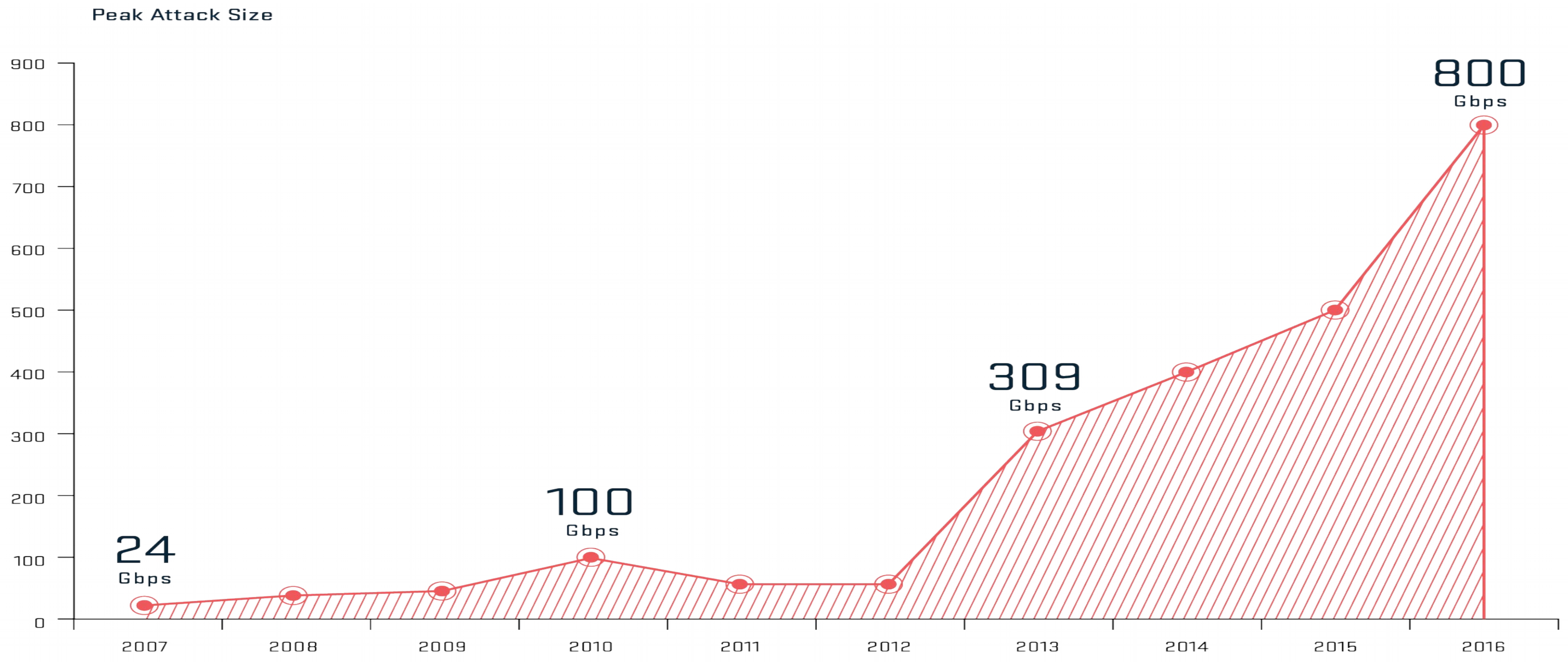


## COMPLEXITY



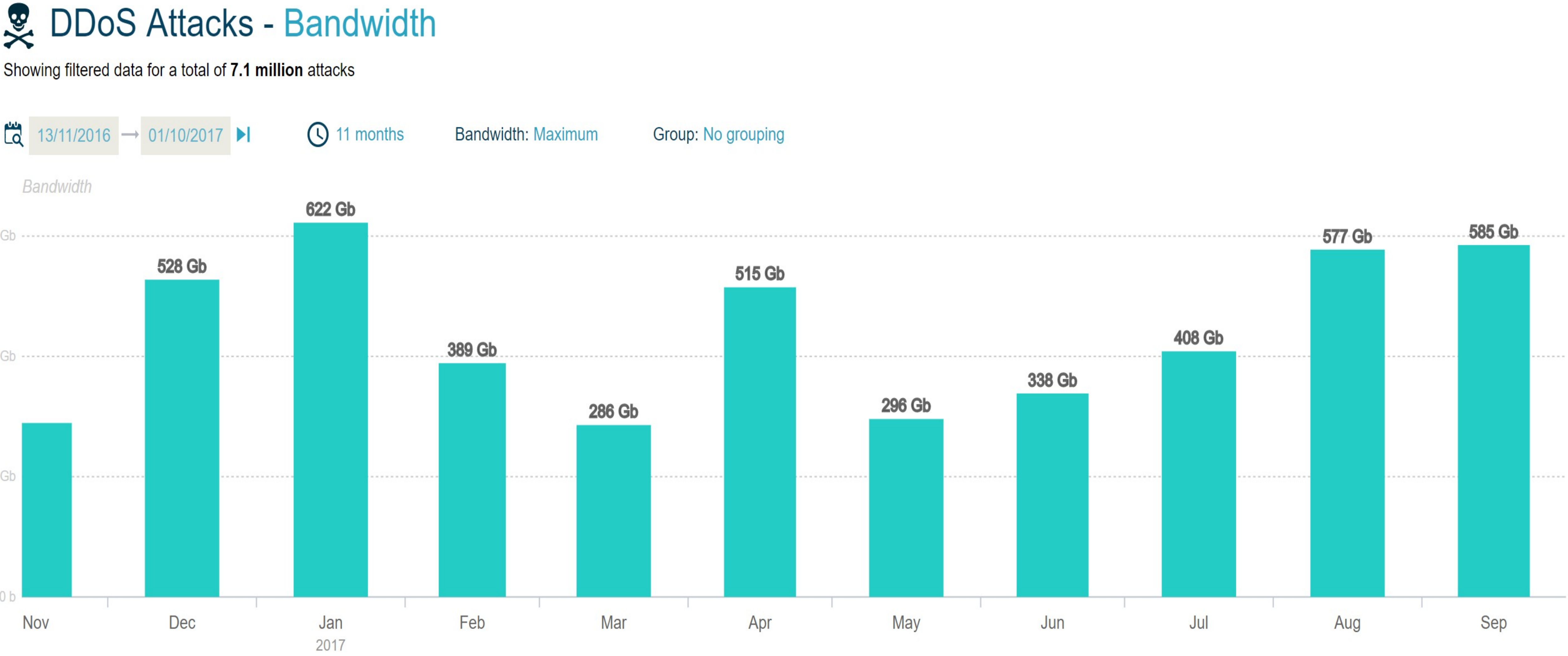
of DDoS Attacks

# DDoS Attacks Increasing in Size



Source: Arbor Networks, Inc.

- Largest attack reported was 800 Gbps with other respondents reporting attacks of 600 Gbps, 550 Gbps, and 500 Gbps
- One third of respondents report peak attacks over 100Gbps
- 41% of EGE respondents and 61% of data-center operators reported attacks exceeding their total Internet capacity



# DDoS Attacks - Bandwidth

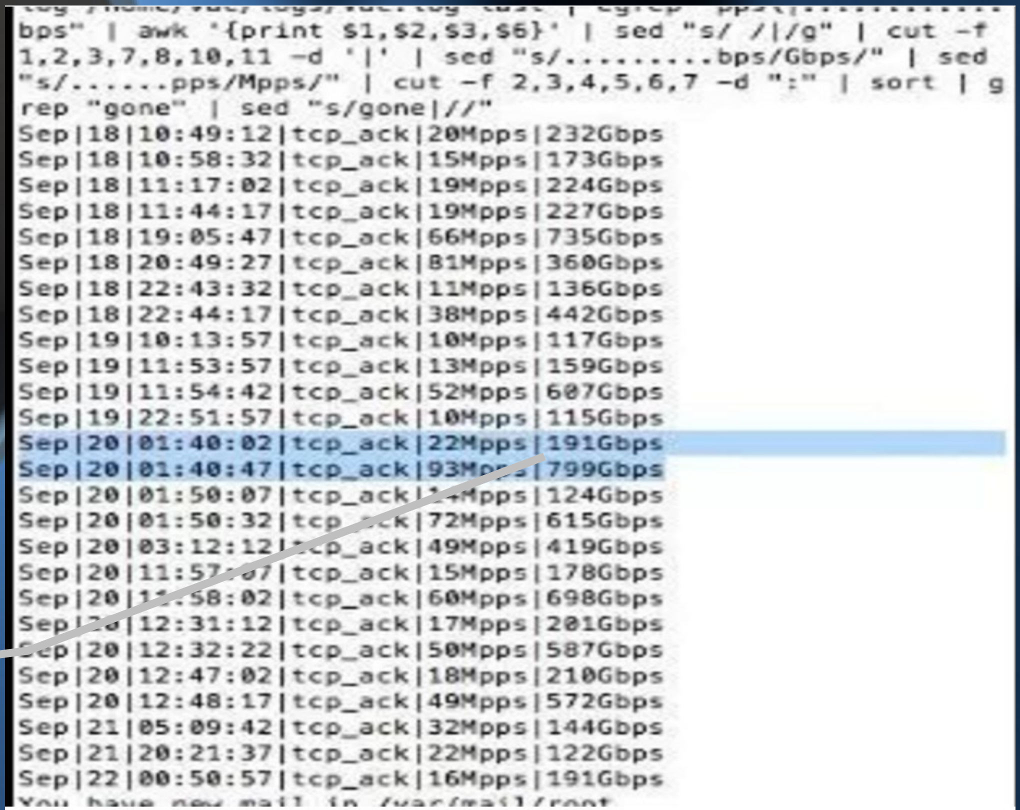
Showing filtered data for a total of **7.1 million** attacks

13/11/2016 → 01/10/2017 ▶| 11 months Bandwidth: Maximum Group: No grouping

NEWS

# Thousands of hacked CCTV devices used in DDoS attacks

Researchers found a botnet of over 25,000 CCTV cameras and digital video recorders

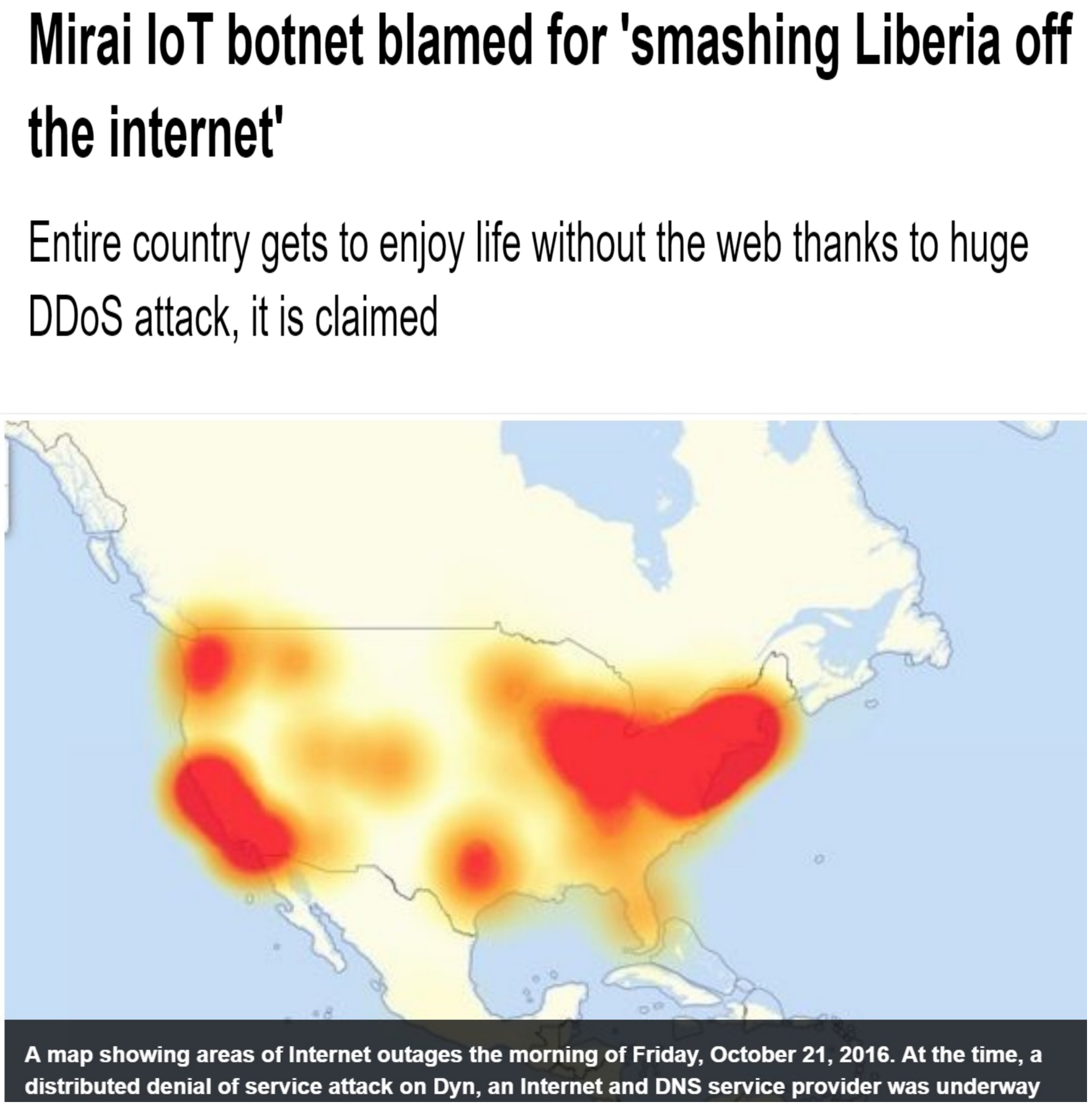


```
bps" | awk '{print $1,$2,$3,$6}' | sed "s/ /|/g" | cut -f
1,2,3,7,8,10,11 -d '|' | sed "s/.........bps/Gbps/" | sed
"s/......pps/Mpps/" | cut -f 2,3,4,5,6,7 -d ":" | sort | g
rep "gone" | sed "s/gone|//"
Sep|18|10:49:12|tcp_ack|20Mpps|232Gbps
Sep|18|10:58:32|tcp_ack|15Mpps|173Gbps
Sep|18|11:17:02|tcp_ack|19Mpps|224Gbps
Sep|18|11:44:17|tcp_ack|19Mpps|227Gbps
Sep|18|19:05:47|tcp_ack|66Mpps|735Gbps
Sep|18|20:49:27|tcp_ack|81Mpps|360Gbps
Sep|18|22:43:32|tcp_ack|11Mpps|136Gbps
Sep|18|22:44:17|tcp_ack|38Mpps|442Gbps
Sep|19|10:13:57|tcp_ack|10Mpps|117Gbps
Sep|19|11:53:57|tcp_ack|13Mpps|159Gbps
Sep|19|11:54:42|tcp_ack|52Mpps|607Gbps
Sep|19|22:51:57|tcp_ack|10Mpps|115Gbps
Sep|20|01:40:02|tcp_ack|22Mpps|191Gbps
Sep|20|01:40:47|tcp_ack|93Mpps|799Gbps
Sep|20|01:50:07|tcp_ack|14Mpps|124Gbps
Sep|20|01:50:32|tcp_ack|72Mpps|615Gbps
Sep|20|03:12:12|tcp_ack|49Mpps|419Gbps
Sep|20|11:57:07|tcp_ack|15Mpps|178Gbps
Sep|20|11:58:02|tcp_ack|60Mpps|698Gbps
Sep|20|12:31:12|tcp_ack|17Mpps|201Gbps
Sep|20|12:32:22|tcp_ack|50Mpps|587Gbps
Sep|20|12:47:02|tcp_ack|18Mpps|210Gbps
Sep|20|12:48:17|tcp_ack|49Mpps|572Gbps
Sep|21|05:09:42|tcp_ack|32Mpps|144Gbps
Sep|21|20:21:37|tcp_ack|22Mpps|122Gbps
Sep|22|00:50:57|tcp_ack|16Mpps|191Gbps
You have new mail in /var/mail/root
```

~ 1Tbps

25,000 CCTV Cameras Hacked

Massive DDoS Attack Launched



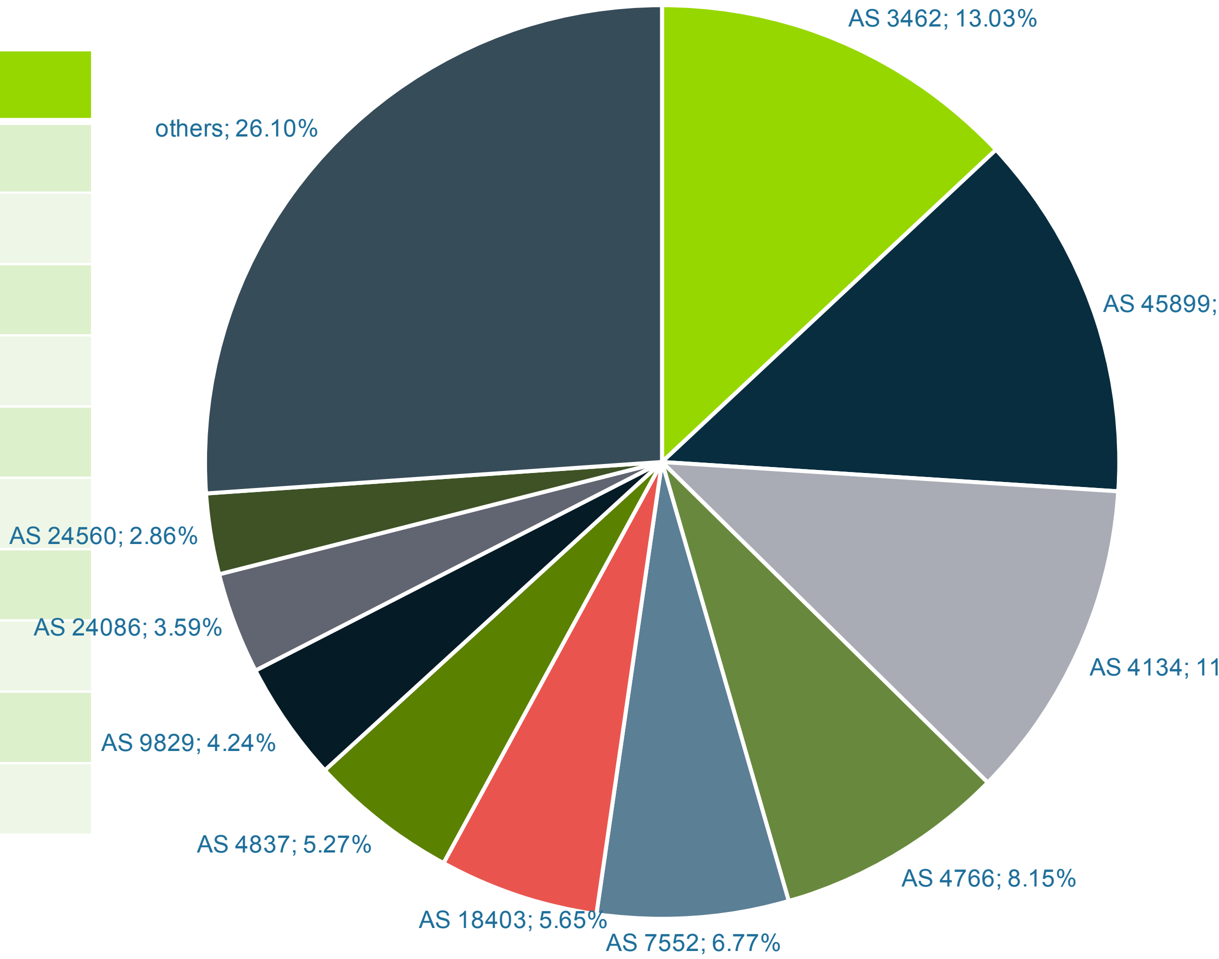
# Mirai IoT botnet blamed for 'smashing Liberia off the internet'

Entire country gets to enjoy life without the web thanks to huge DDoS attack, it is claimed

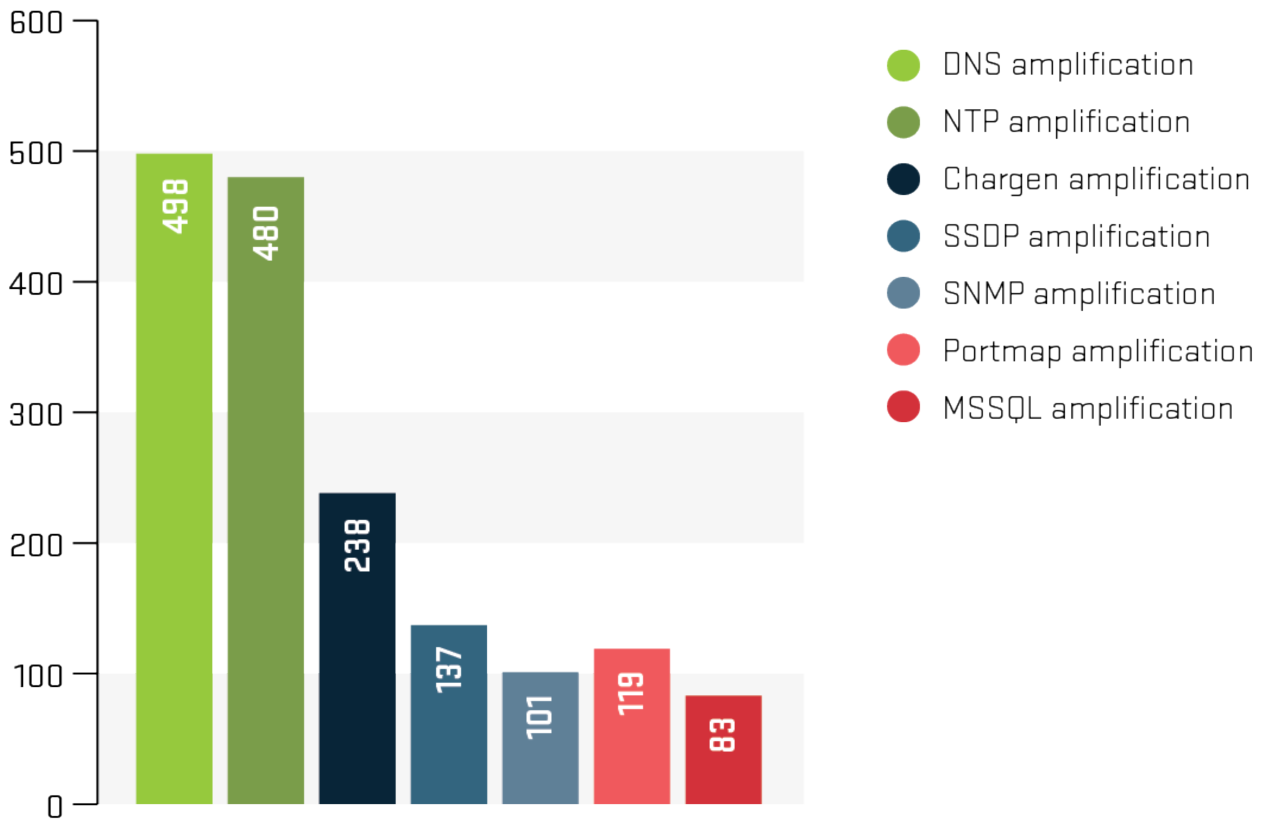
A map showing areas of Internet outages the morning of Friday, October 21, 2016. At the time, a distributed denial of service attack on Dyn, an Internet and DNS service provider was underway

| Country | Number of Attempts |
|---|---|
| China | 102,975 |
| Vietnam | 26,573 |
| Republic of Korea | 19,465 |
| USA | 17,062 |
| Brazil | 16,609 |
| Russia | 13,378 |
| Taiwan | 11,697 |
| Hong Kong | 11,200 |
| Turkey | 10,190 |
| Romania | 9,856 |

## Login attempts by APAC ASN



ATLAS Reflection/Amplification Attacks, Peak Sizes (Gbps)



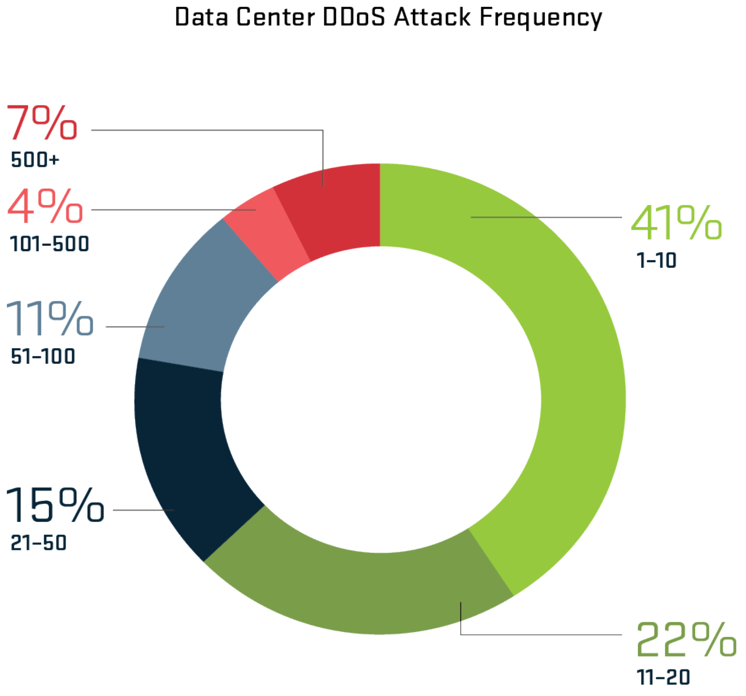
Source: Arbor Networks, Inc.

- Reflection Amplification attacks continue, but there has been some cyclic change in the protocols favored by attackers.
- Strong growth in the use of DNS (again) through 2016
- Largest monitored attack of 498.3Gbs, a 97% jump from last year
  - DNS and NTP attacks over 400Gbps, Chargen over 200Gbps

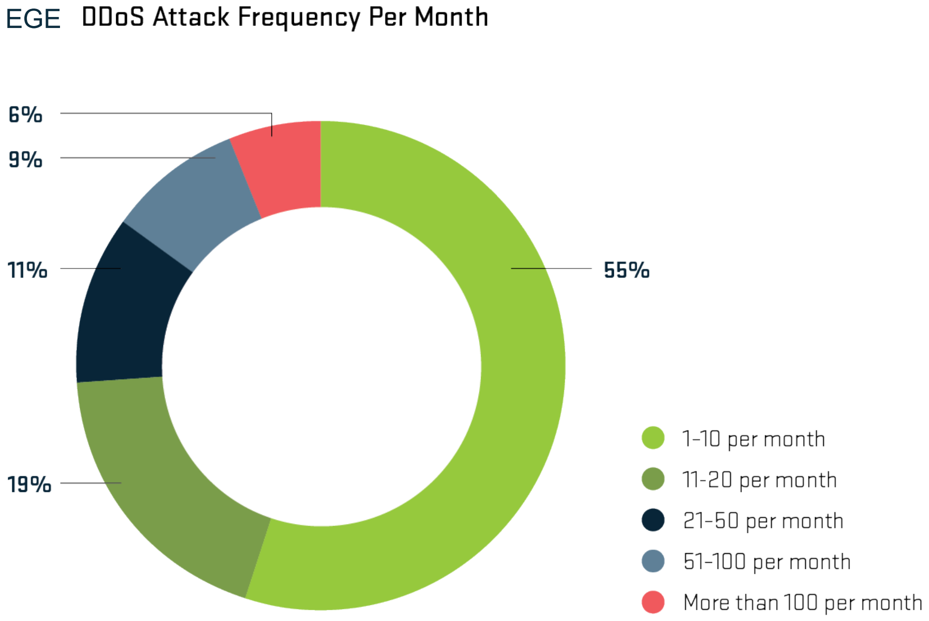
# 1 Every 6 Seconds

## DDoS Attacks

ARBOR NETWORKS
The Security Division of NETSCOUT

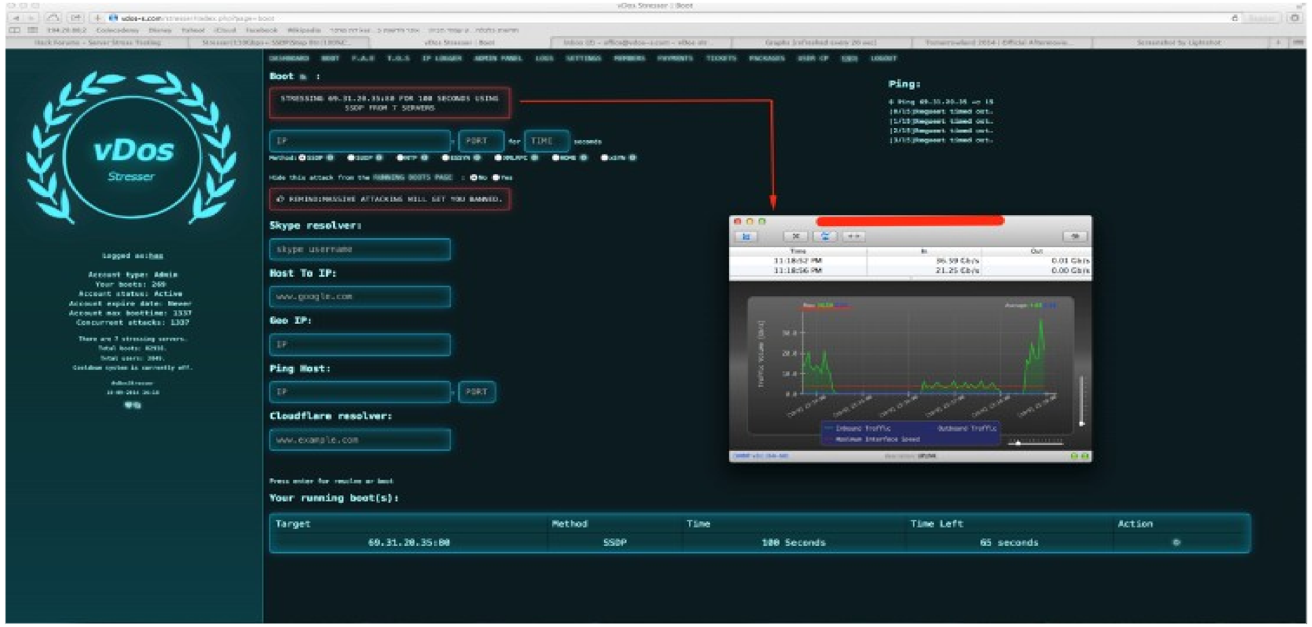


Source: Arbor Networks, Inc.



Source: Arbor Networks, Inc.

- 53% of SPs see more than 51 attacks per month, up from 44%
- 21% of data-centers see more than 50 attacks per month, up from 8%
- 45% of EGE see more than 10 attacks per month, up from 28%
- ATLAS is tracking 135,000 Volumetric attacks per week.



vDos Stresser :: Boot

Boot :

```
STRESSING 69.31.20.35:80 FOR 100 SECONDS USING
SSDP FROM 7 SERVERS
```

IP : PORT for TIME seconds

REMIND:MASSIVE ATTACKING WILL GET YOU BANNED.

Skype resolver:

Host To IP:

Geo IP:

Ping Host:

Cloudflare resolver:

Press enter for resolve or boot

Your running boot(s):

| Target | Method | Time | Time Left | Action |
|---|---|---|---|---|
| 69.31.20.35:80 | SSDP | 100 Seconds | 65 seconds | |

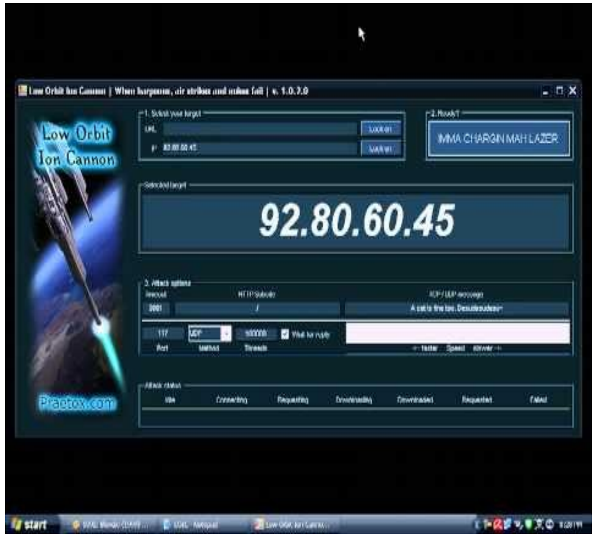
```
Logged as:

Account type: Admin
Your boots: 269
Account status: Active
Account expire date: Never
Account max boottime: 1337
Concurrent attacks: 1337

There are 7 stressing servers.
```

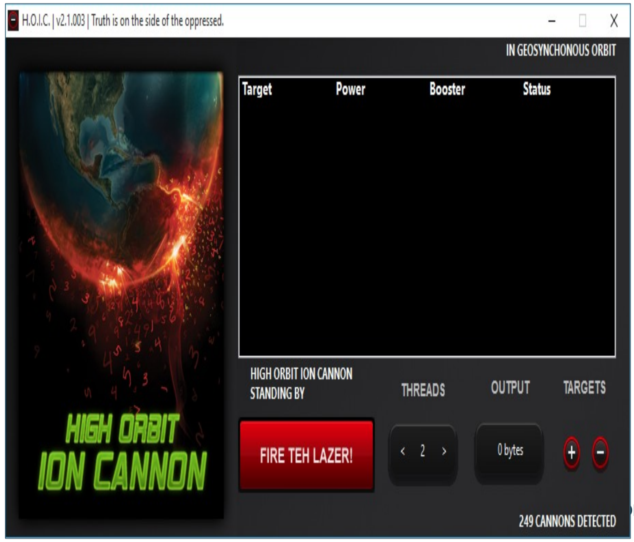
Ping:

```
|[illegible]Request timed out.
|[illegible]Request timed out.
|[illegible]Request timed out.
|[illegible]Request timed out.
```



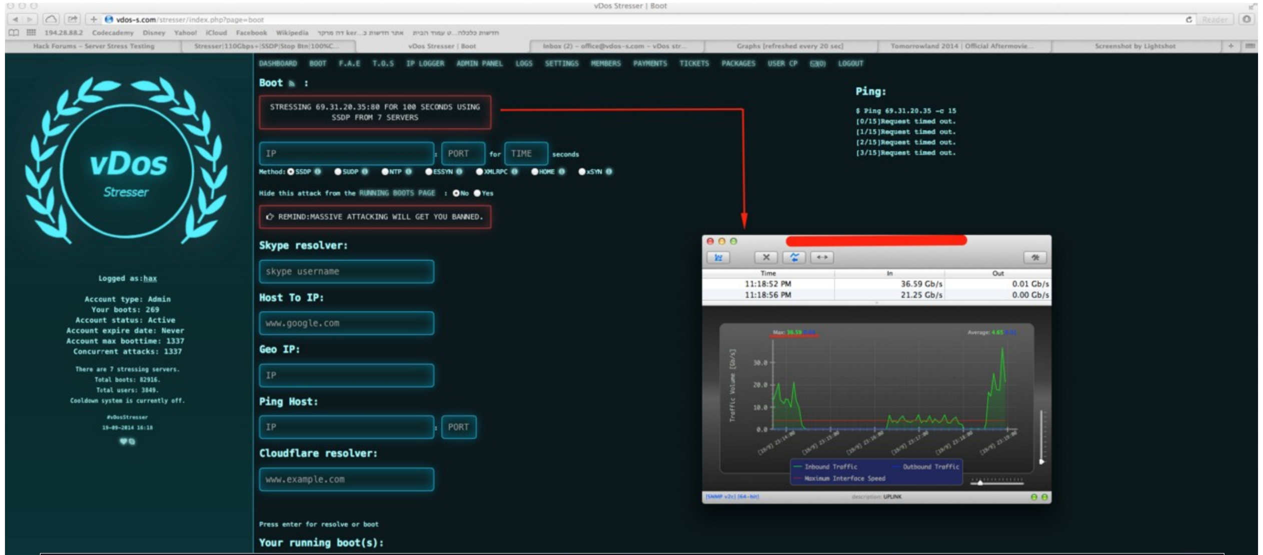
Low Orbit Ion Cannon | When harpoons, air strikes and nukes fail | v. 1.0.7.0

Selected target: 92.80.60.45



H.O.I.C. | v2.1.003 | Truth is on the side of the oppressed.

# Frequency - DDoS tools for the masses


vDos Stresser | Boot
vdos-s.com/stresser/index.php?page=boot
194.28.88.2 Codecademy Disney Yahoo! iCloud Facebook Wikipedia
Hack Forums - Server Stress Testing
Stresser|110Gbps+|SSDP|Stop Btn|100%C...
vDos Stresser | Boot
Inbox (2) - office@vdos-s.com - vDos str...
Graphs [refreshed every 20 sec]
Tomorrowland 2014 | Official Aftermovie...
Screenshot by Lightshot
DASHBOARD BOOT F.A.E T.O.S IP LOGGER ADMIN PANEL LOGS SETTINGS MEMBERS PAYMENTS TICKETS PACKAGES USER CP (0) LOGOUT
vDos
Stresser

Logged as:hax

Account type: Admin
Your boots: 269
Account status: Active
Account expire date: Never
Account max boottime: 1337
Concurrent attacks: 1337

There are 7 stressing servers.
Total boots: 82916.
Total users: 3849.
Cooldown system is currently off.

#vDosStresser
19-09-2014 16:18

Boot :

STRESSING 69.31.20.35:80 FOR 100 SECONDS USING SSDP FROM 7 SERVERS

IP : PORT for TIME seconds

Method: ● SSDP ○ SUDP ○ NTP ○ ESSYN ○ XMLRPC ○ HOME ○ xSYN

Hide this attack from the RUNNING BOOTS PAGE : ● No ○ Yes

REMIND:MASSIVE ATTACKING WILL GET YOU BANNED.

Skype resolver:

skype username

Host To IP:

www.google.com

Geo IP:

IP

Ping Host:

IP : PORT

Cloudflare resolver:

www.example.com

Press enter for resolve or boot

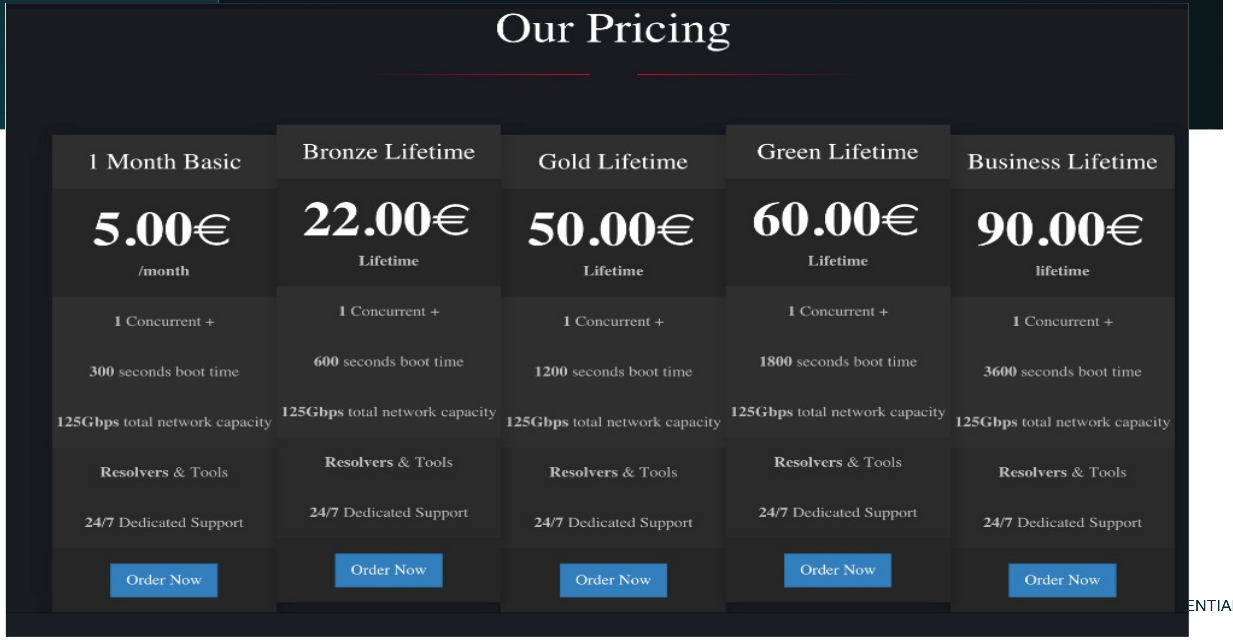
Your running boot(s):

Ping:

```
$ Ping 69.31.20.35 -c 15
[0/15]Request timed out.
[1/15]Request timed out.
[2/15]Request timed out.
[3/15]Request timed out.
```

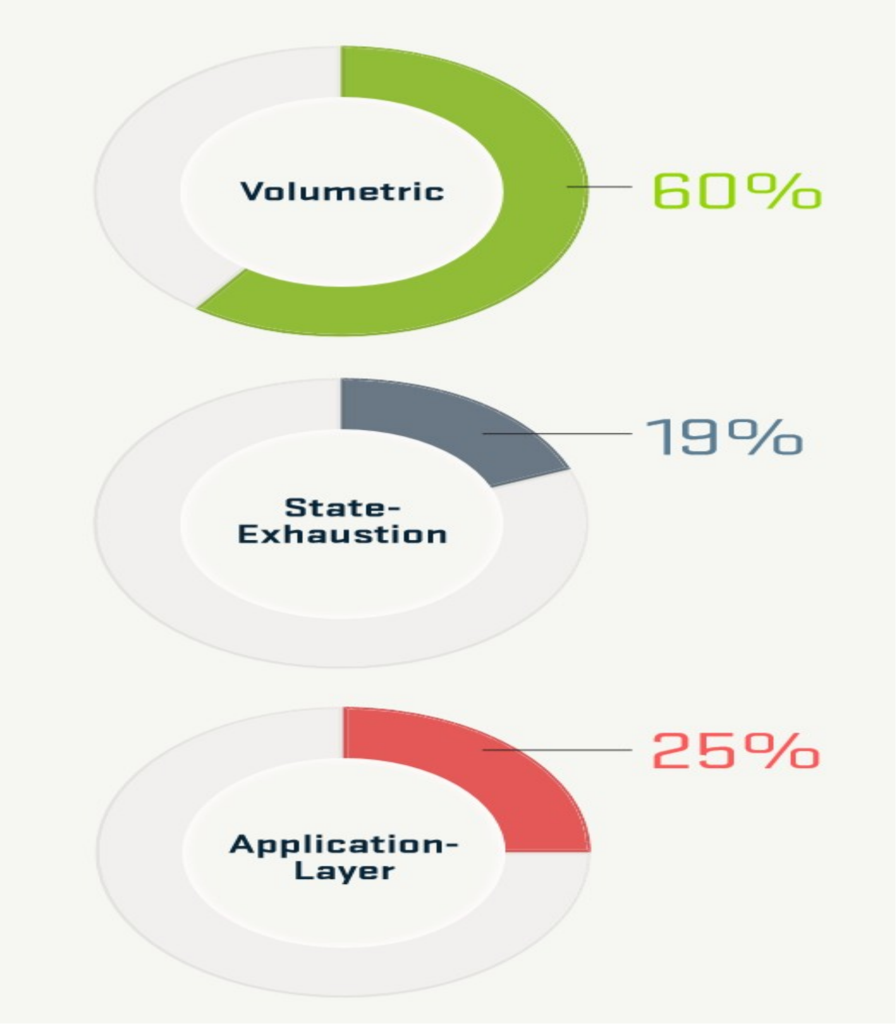
[redacted]

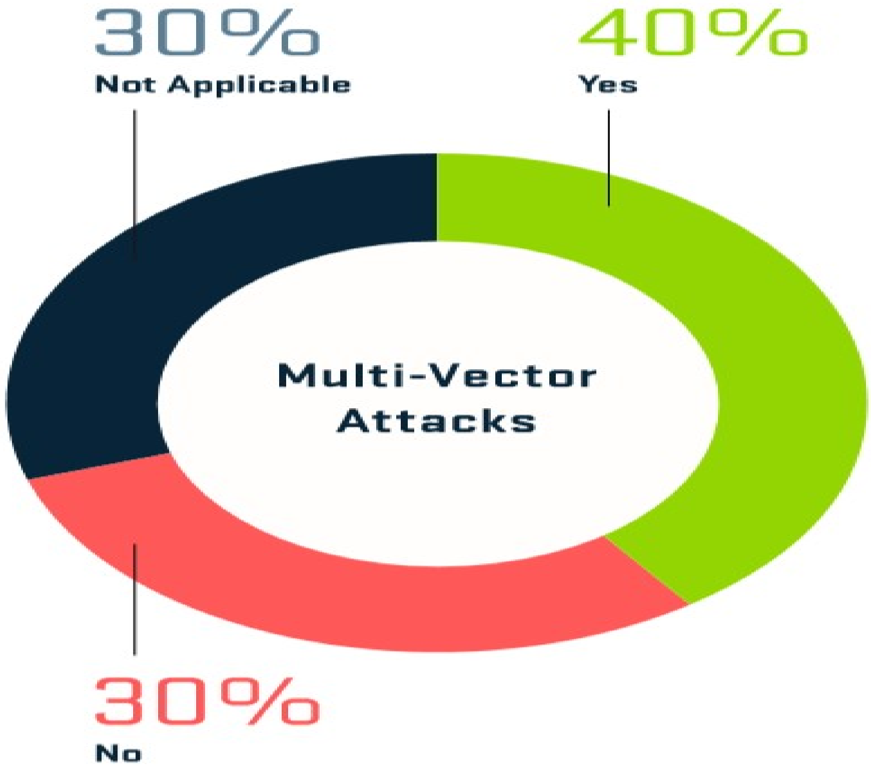
| Time | In | Out |
|---|---|---|
| 11:18:52 PM | 36.59 Gb/s | 0.01 Gb/s |
| 11:18:56 PM | 21.25 Gb/s | 0.00 Gb/s |

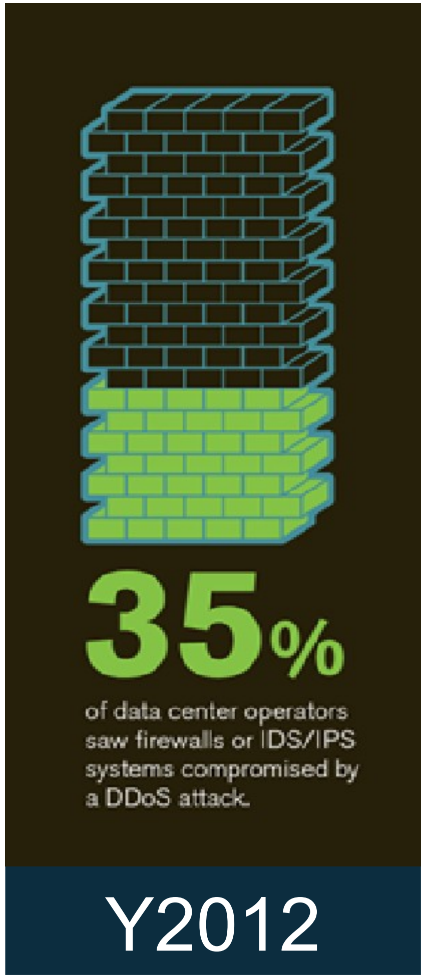


## Our Pricing

| 1 Month Basic | Bronze Lifetime | Gold Lifetime | Green Lifetime | Business Lifetime |
|---|---|---|---|---|
| 5.00€<br>/month | 22.00€<br>Lifetime | 50.00€<br>Lifetime | 60.00€<br>Lifetime | 90.00€<br>lifetime |
| 1 Concurrent + | 1 Concurrent + | 1 Concurrent + | 1 Concurrent + | 1 Concurrent + |
| 300 seconds boot time | 600 seconds boot time | 1200 seconds boot time | 1800 seconds boot time | 3600 seconds boot time |
| 125Gbps total network capacity | 125Gbps total network capacity | 125Gbps total network capacity | 125Gbps total network capacity | 125Gbps total network capacity |
| Resolvers & Tools | Resolvers & Tools | Resolvers & Tools | Resolvers & Tools | Resolvers & Tools |
| 24/7 Dedicated Support | 24/7 Dedicated Support | 24/7 Dedicated Support | 24/7 Dedicated Support | 24/7 Dedicated Support |
| Order Now | Order Now | Order Now | Order Now | Order Now |

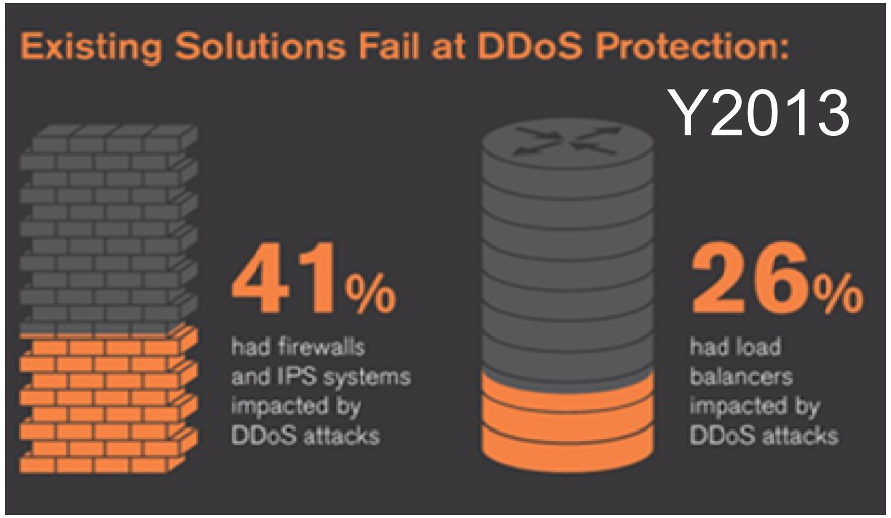

Volumetric
60%
State-Exhaustion
19%
Application-Layer
25%


30%
Not Applicable
40%
Yes
Multi-Vector Attacks
30%
No



35% of data center operators saw firewalls or IDS/IPS systems compromised by a DDoS attack.

Y2012

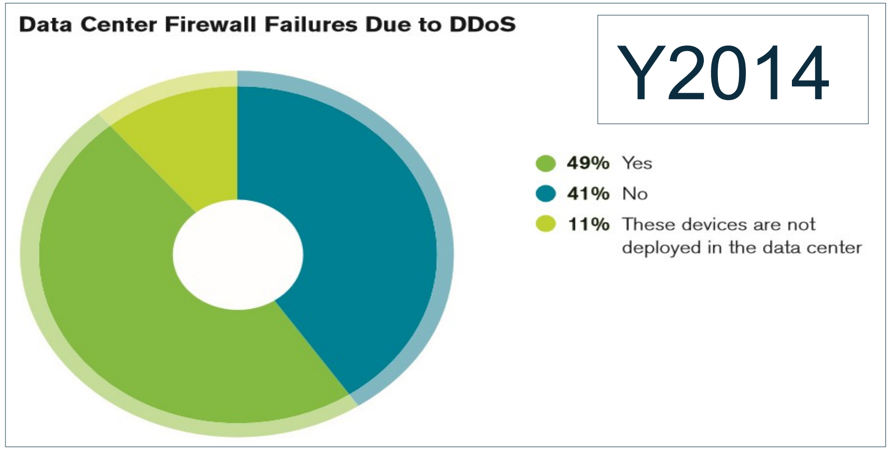


Existing Solutions Fail at DDoS Protection:

Y2013

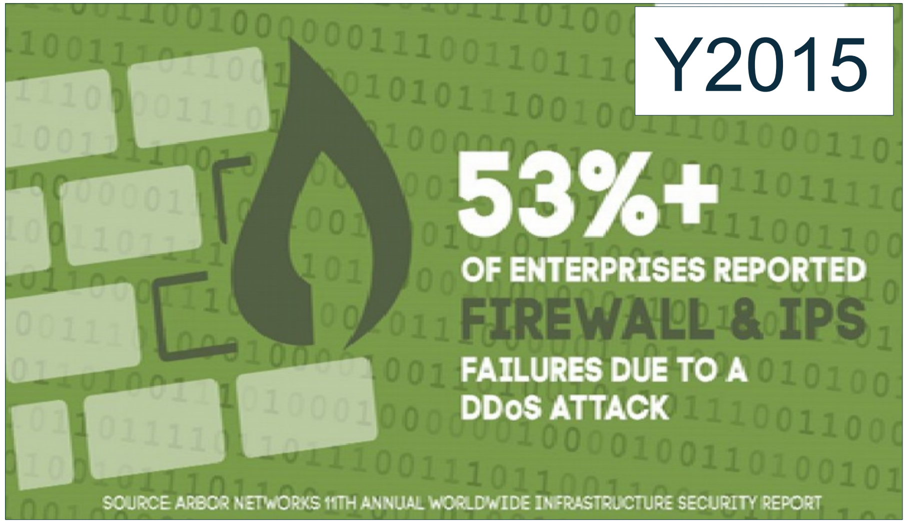
41% had firewalls and IPS systems impacted by DDoS attacks

26% had load balancers impacted by DDoS attacks



Data Center Firewall Failures Due to DDoS

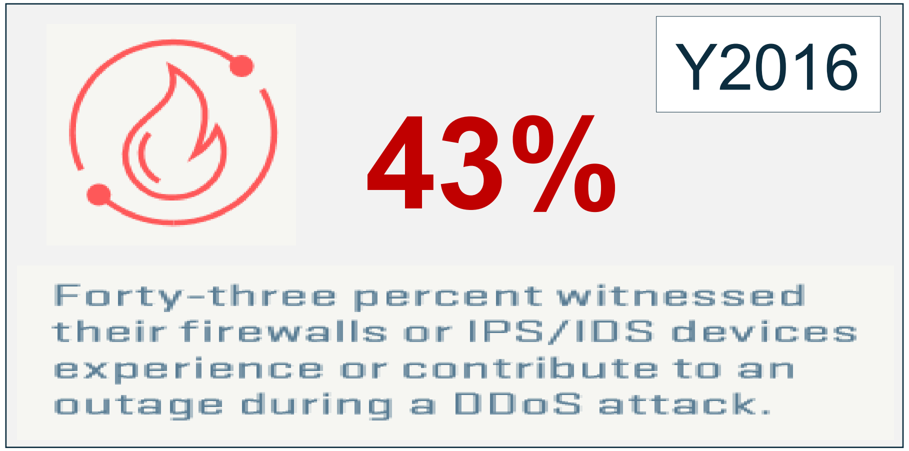
Y2014



Y2015

53%+ OF ENTERPRISES REPORTED FIREWALL & IPS FAILURES DUE TO A DDoS ATTACK

SOURCE: ARBOR NETWORKS 11TH ANNUAL WORLDWIDE INFRASTRUCTURE SECURITY REPORT



Y2016

43%

Forty-three percent witnessed their firewalls or IPS/IDS devices experience or contribute to an outage during a DDoS attack.

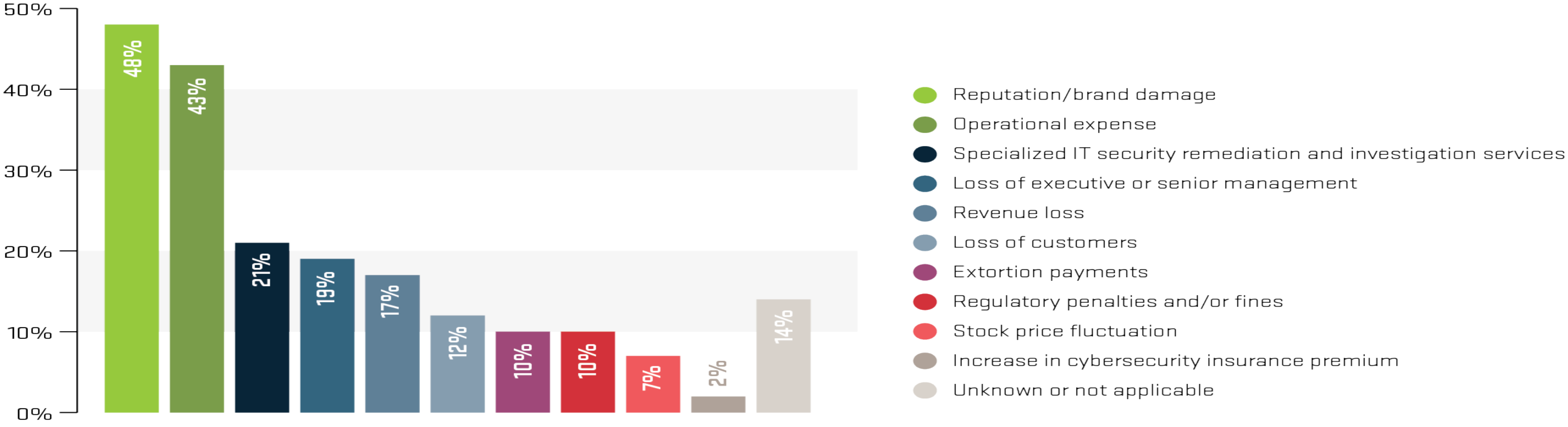
Source: Arbor Networks Annual Worldwide Infrastructure Security Report

## Attack Target Customer Verticals

| | |
|---|---|
| 69% | End-User/Subscriber |
| 48% | Government |
| 41% | Financial Services |
| 40% | Hosting |
| 36% | eCommerce |
| 35% | Gaming |
| 31% | Education |
| 13% | Law Enforcement |
| 10% | Healthcare |
| 10% | Energy/Utilities |
| 9% | Gambling |
| 7% | Manufacturing |
| 7% | Other |

Source: Arbor Networks, Inc.

Business Impacts of DDoS Attacks



Source: Arbor Networks, Inc.

- Reputation/brand damage and operational expense most commonly cited business impacts by EGE respondents
  - Increase from 36% to 48% experiencing brand damage
- 59% of EGE respondents estimate downtime cost of > $500/min.
- Majority estimate cost of a major attack below $10K, some estimate over $1M

**Tony Teo – tteo@arbor.net**
Director Sale Engineering, APJ
Arbor Networks, a Netscout Company

ARBOR® NETWORKS
The Security Division of NETSCOUT