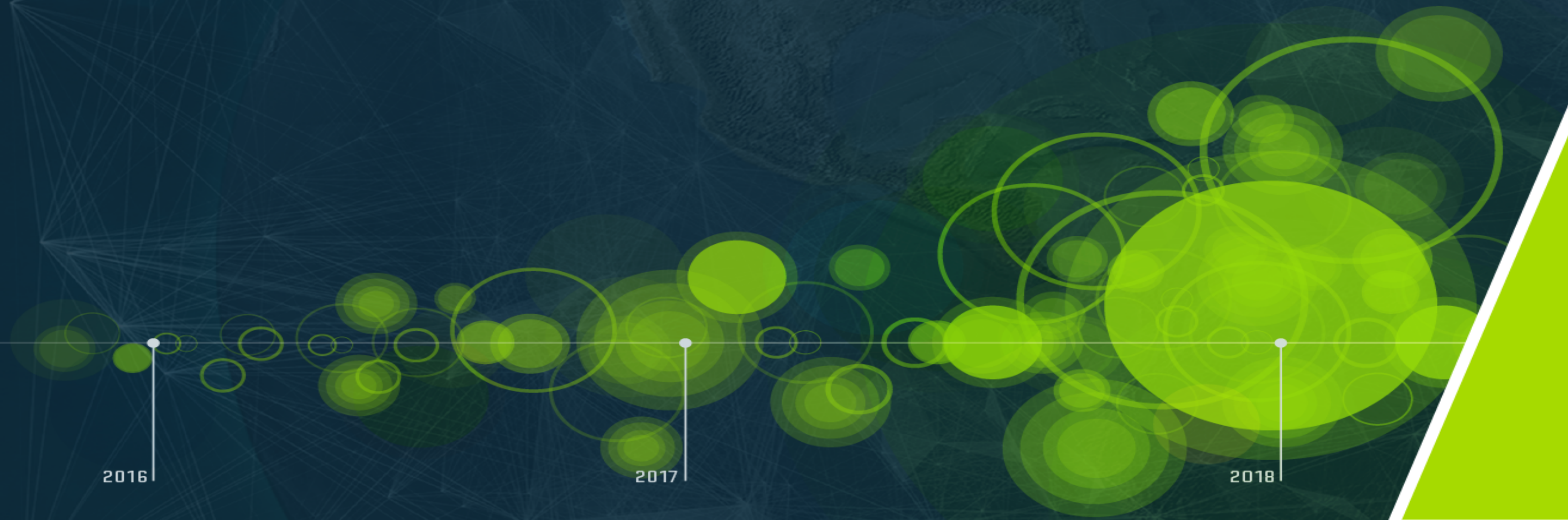
ARBOR NETWORKS

The Security Division of NETSCOUT

The Stakes Have Changed

The Changing Security Landscape



or Security Engineering Respond Team (ASERT) : ATLAS Sens

flow SP
Peakflow X
ISP NET
S DA
ATLAS ANALYSIS SYSTEMS
ARBOR SERT
Security Engineering & Response Team
ATLAS PUBLIC PORTAL

330+ Se

1.76M
dresses

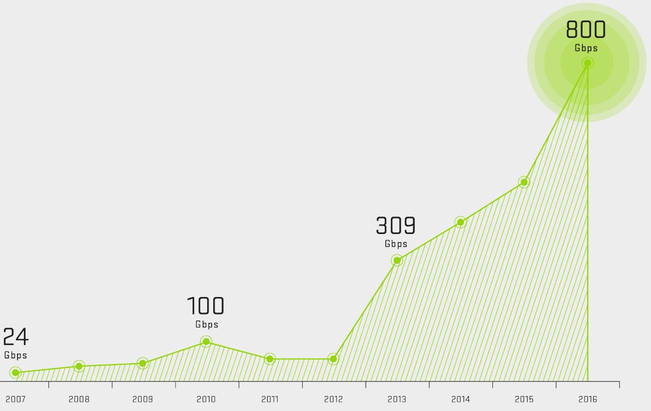
~ 50% Co
National CERT tean

es
71% tical)

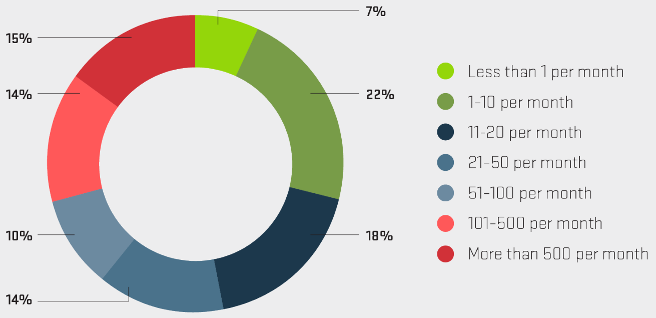
140+ Tbps
(Around 33% of Daily World Internet Traffic)

he Stakes Have Changed

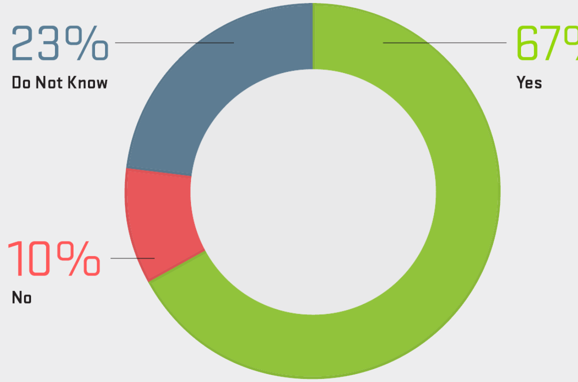
SIZE



FREQUENCY

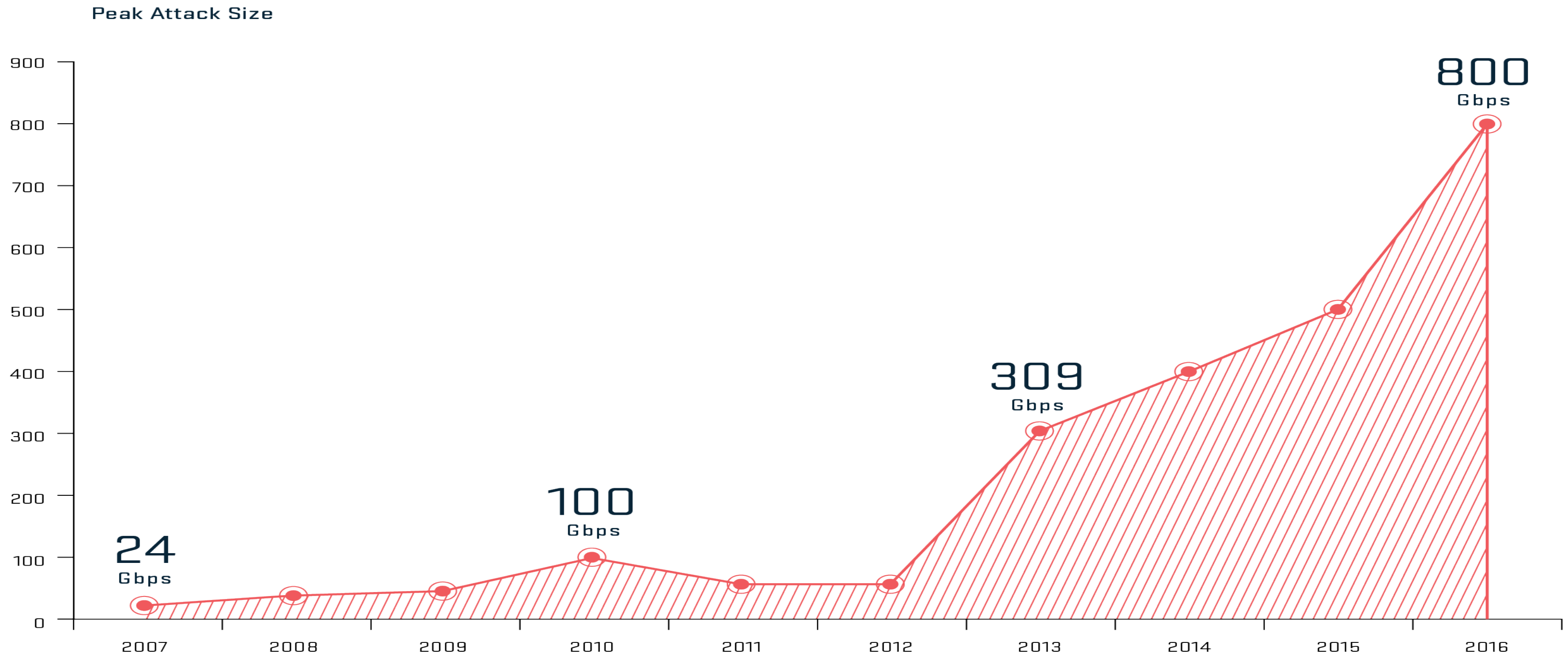


COMPLEXITY



of DDoS Attacks

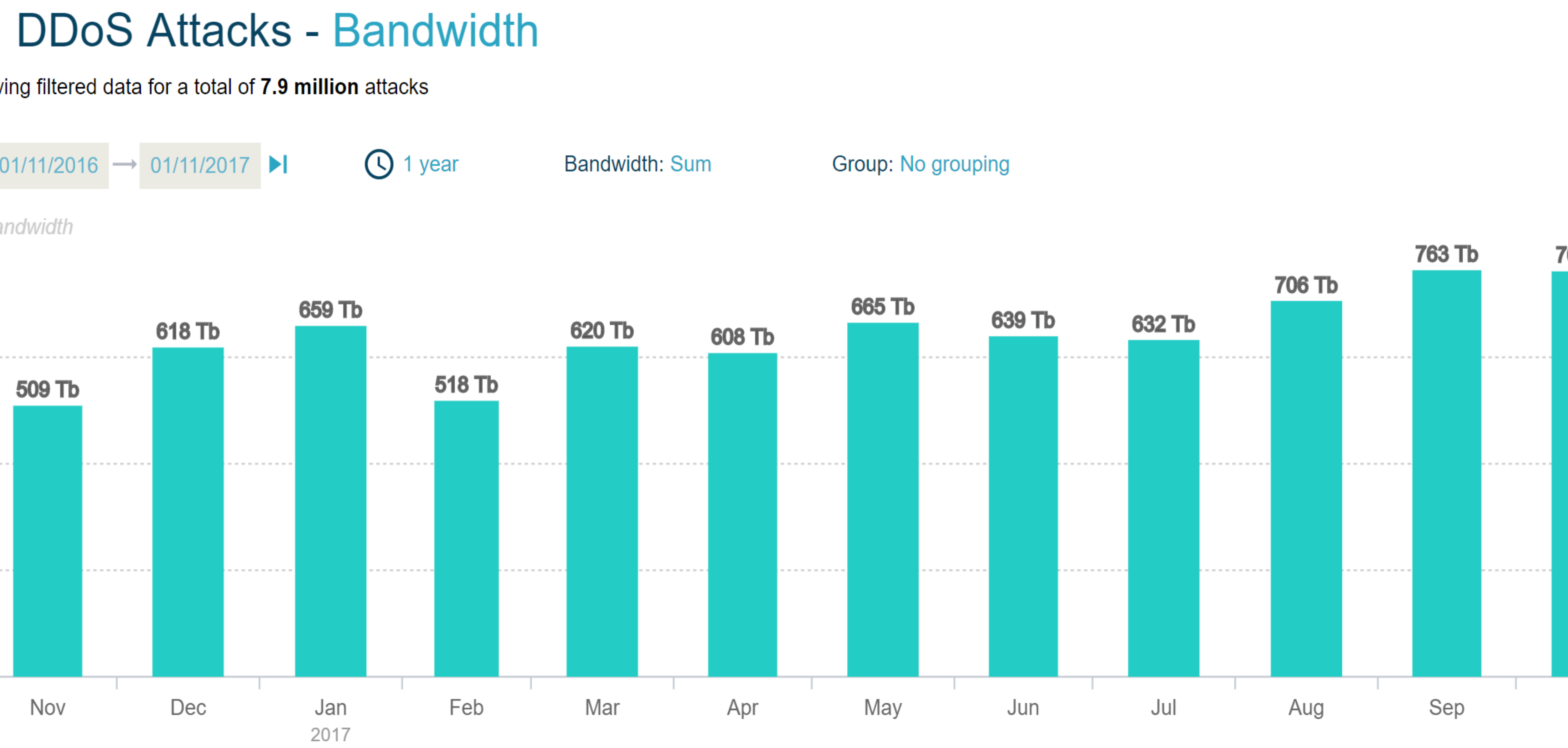
DoS Attacks Increasing in Size



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

orldwide DDoS Attack (Past Year) – Largest DDoS



DDoS Attacks - Bandwidth

ving filtered data for a total of **7.9 million** attacks

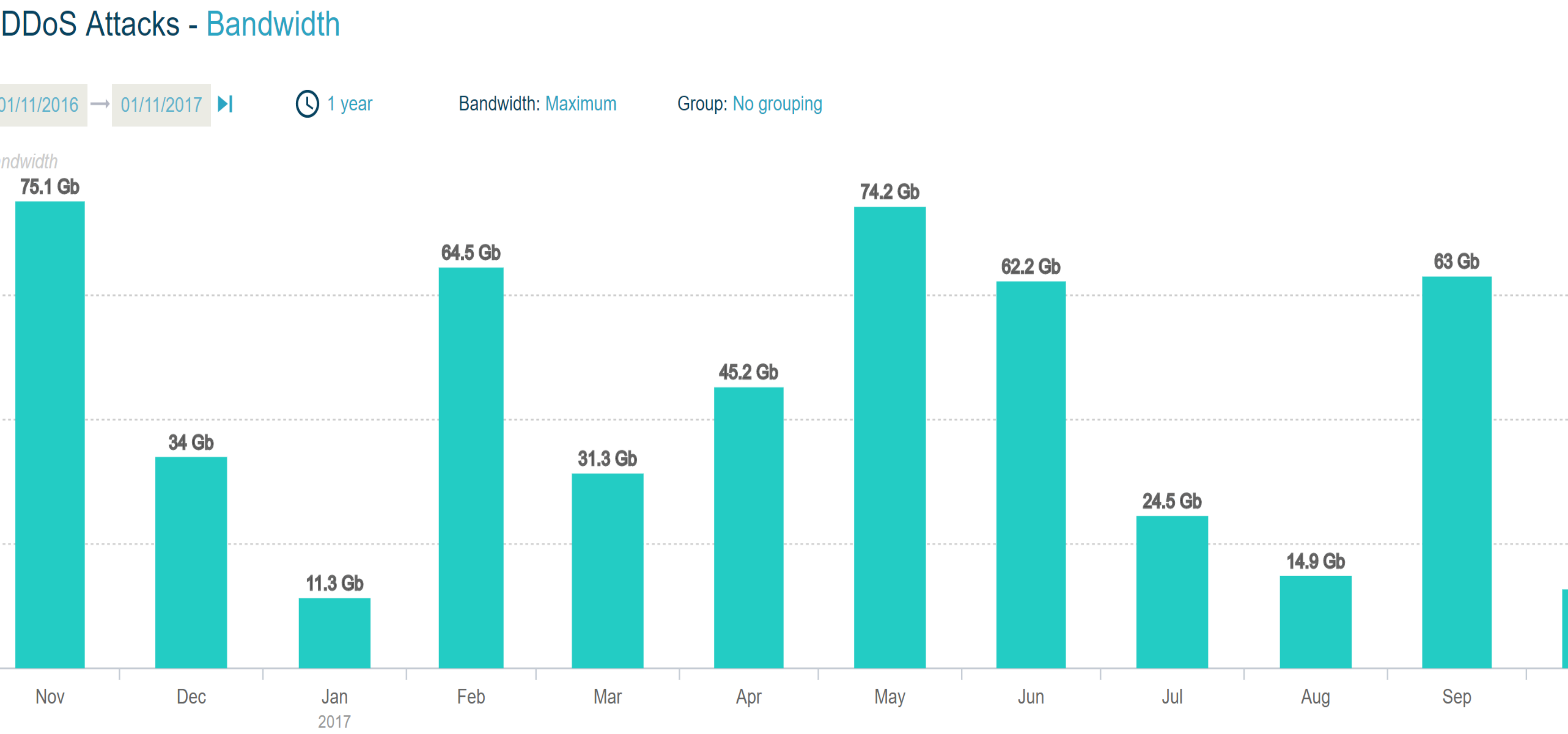
01/11/2016 → 01/11/2017

1 year

Bandwidth: Sum

Group: No grouping

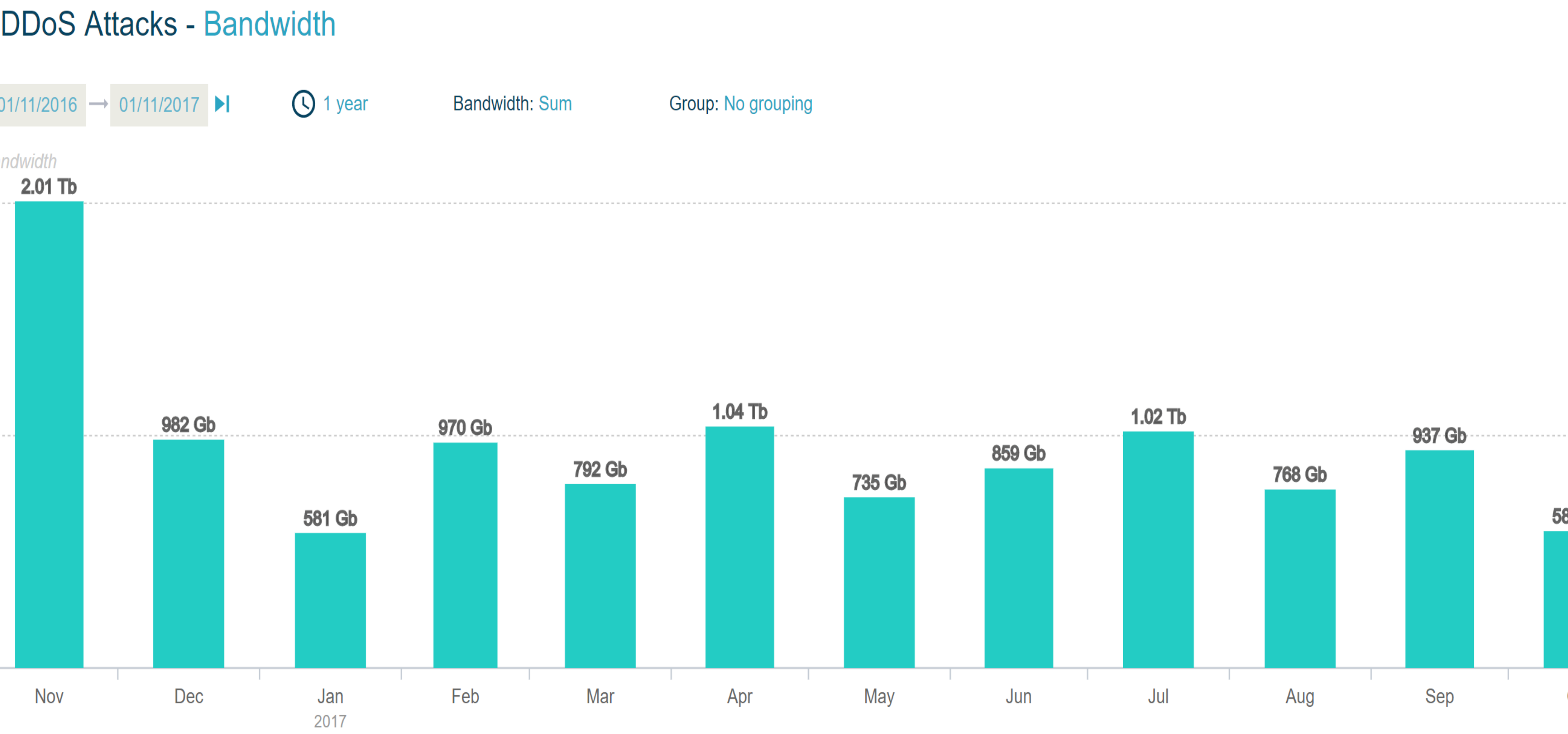
alaysia DDoS Attack (Past Year) – Largest DDoS



DDoS Attacks - Bandwidth

01/11/2016 → 01/11/2017 ▶| 1 year Bandwidth: Maximum Group: No grouping

alaysia DDoS Attack (Past Year) – Total DDoS



DDoS Attacks - Bandwidth

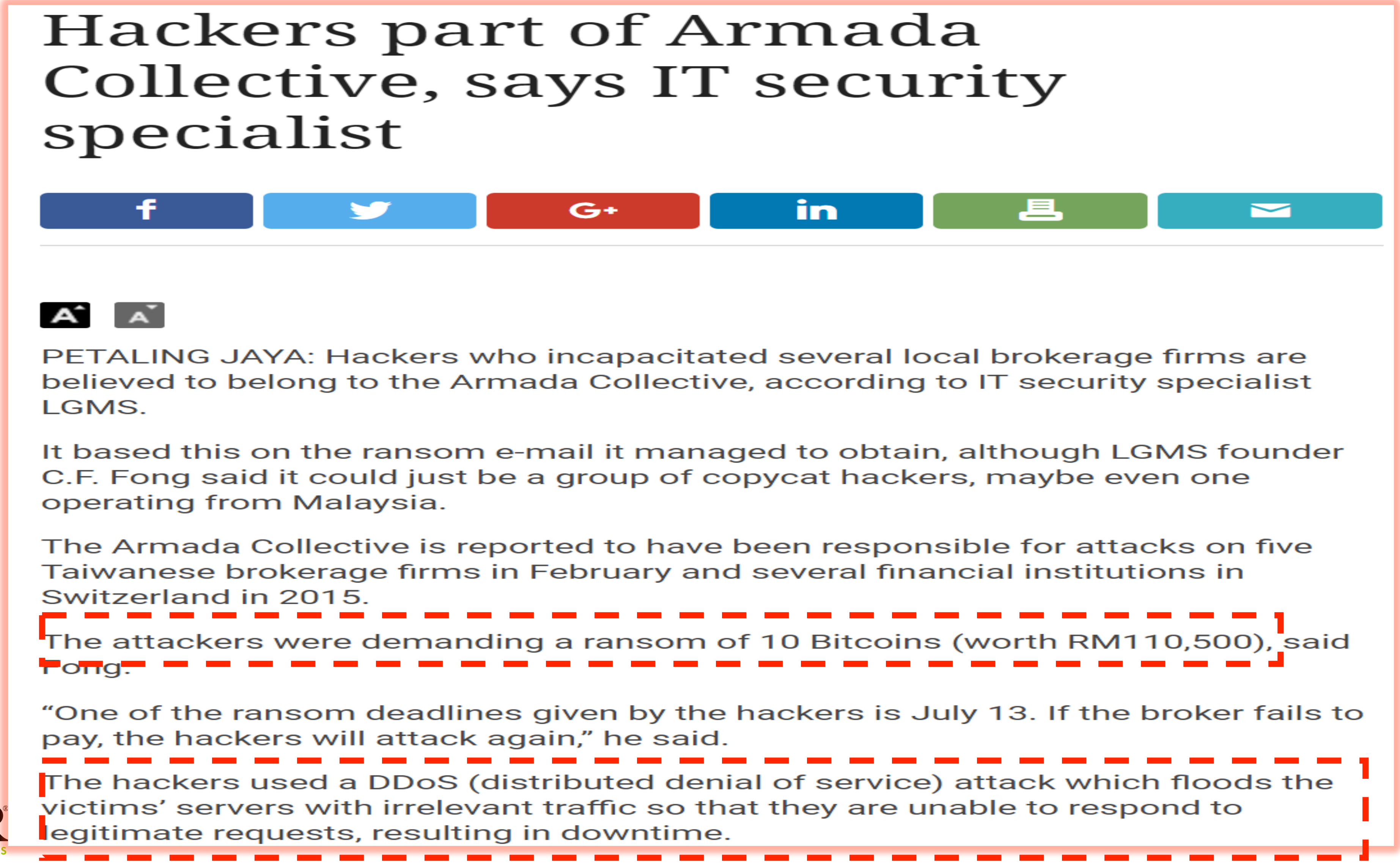
01/11/2016 → 01/11/2017

1 year

Bandwidth: Sum

Group: No grouping

DoS Extortion – Recent Malaysia Attacks



Hackers part of Armada Collective, says IT security specialist

PETALING JAYA: Hackers who incapacitated several local brokerage firms are believed to belong to the Armada Collective, according to IT security specialist LGMS.

It based this on the ransom e-mail it managed to obtain, although LGMS founder C.F. Fong said it could just be a group of copycat hackers, maybe even one operating from Malaysia.

The Armada Collective is reported to have been responsible for attacks on five Taiwanese brokerage firms in February and several financial institutions in Switzerland in 2015.

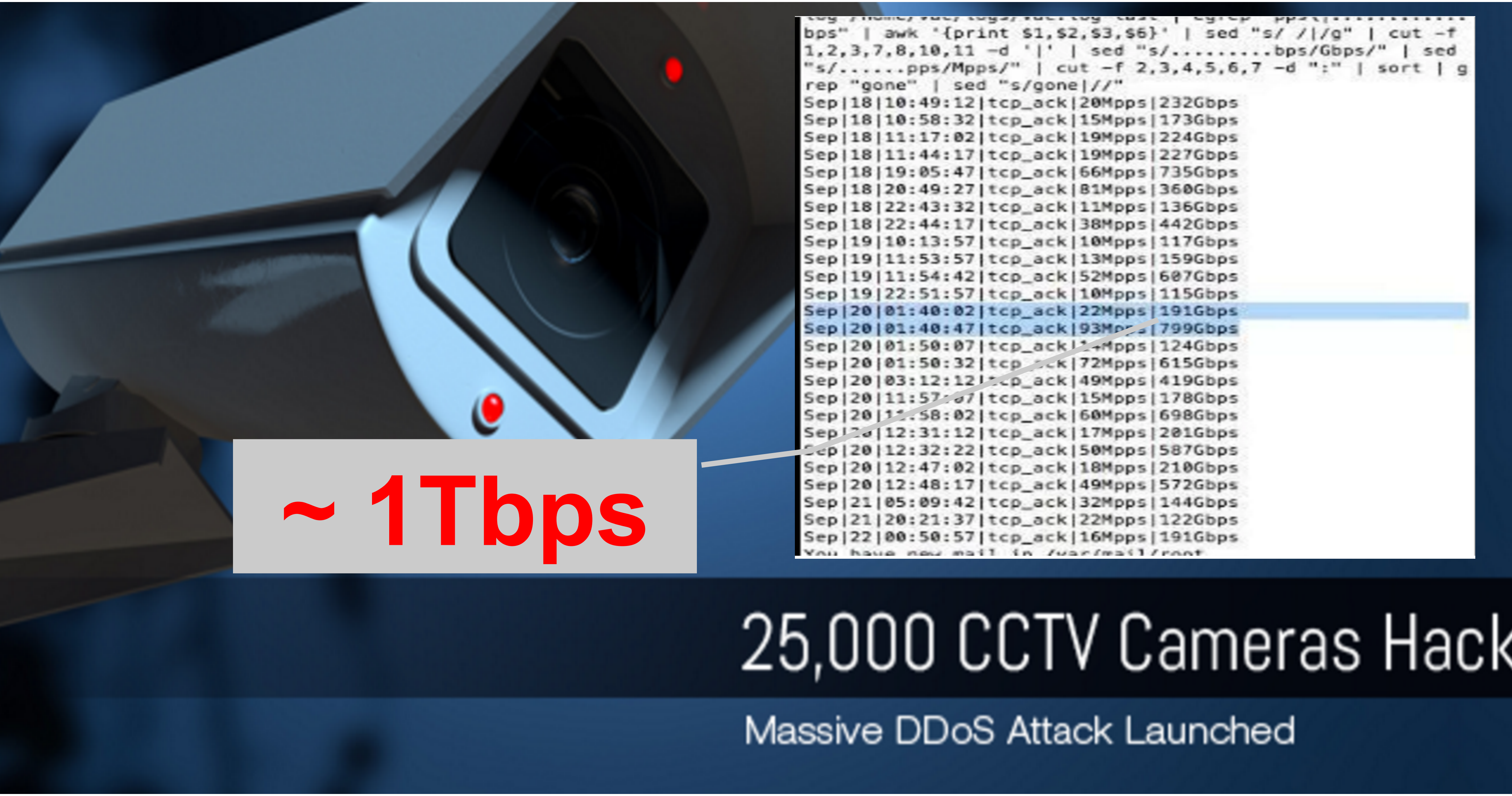
The attackers were demanding a ransom of 10 Bitcoins (worth RM110,500), said Fong.

“One of the ransom deadlines given by the hackers is July 13. If the broker fails to pay, the hackers will attack again,” he said.

The hackers used a DDoS (distributed denial of service) attack which floods the victims’ servers with irrelevant traffic so that they are unable to respond to legitimate requests, resulting in downtime.

housands of hacked CCTV devices used in DDo tacks

earchers 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

2016 IOT Botnet DDoS Attacks

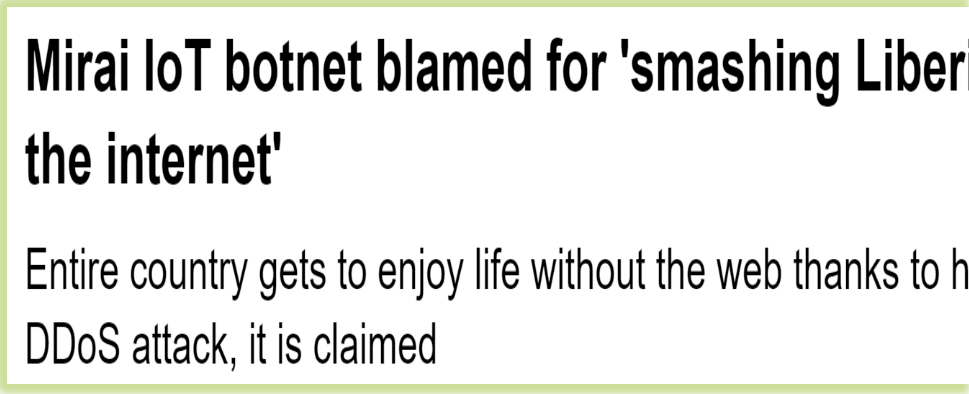
nmer, 2016 – 540 Gbps attack on an organization associated with the Rio Olympics **(Lizardstresser)**

otember 20th – 620 Gbps attack targeting KrebsOnSecurity.com **(Mirai)**

otember 21st – 990 Gbps attack targeting OVH **(Mirai)**

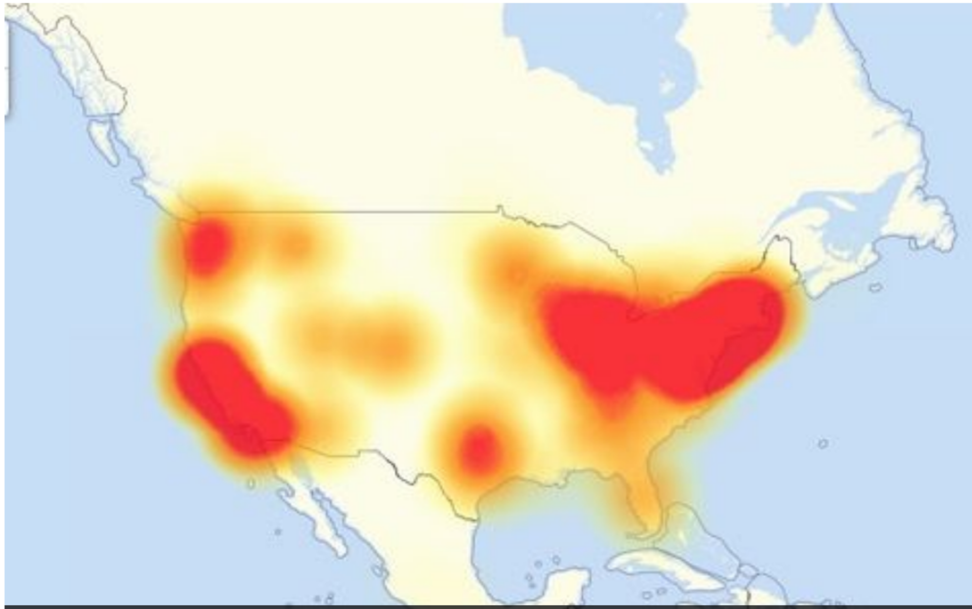
ober 21st – Dyn's Managed DNS Infrastructure Targeted **(Mirai)**

ober 31st – 600 Gbps attack on Liberia **(Mirai)**

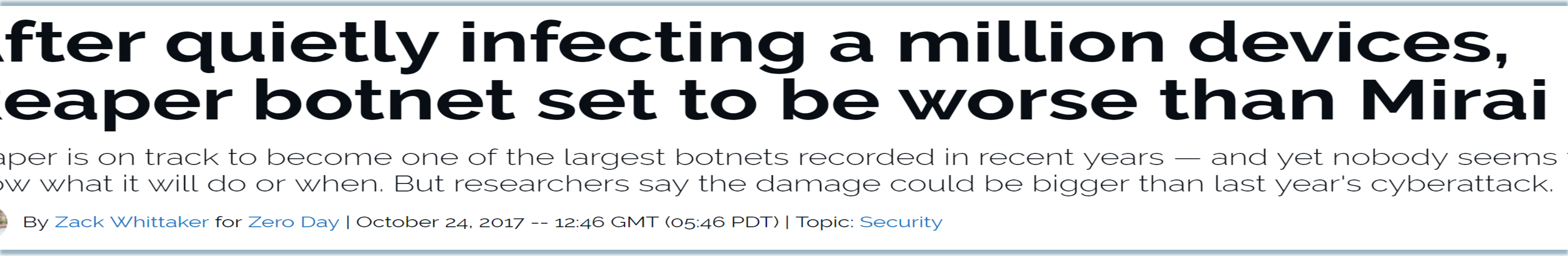


Mirai IoT botnet blamed for 'smashing Liberi the internet'

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



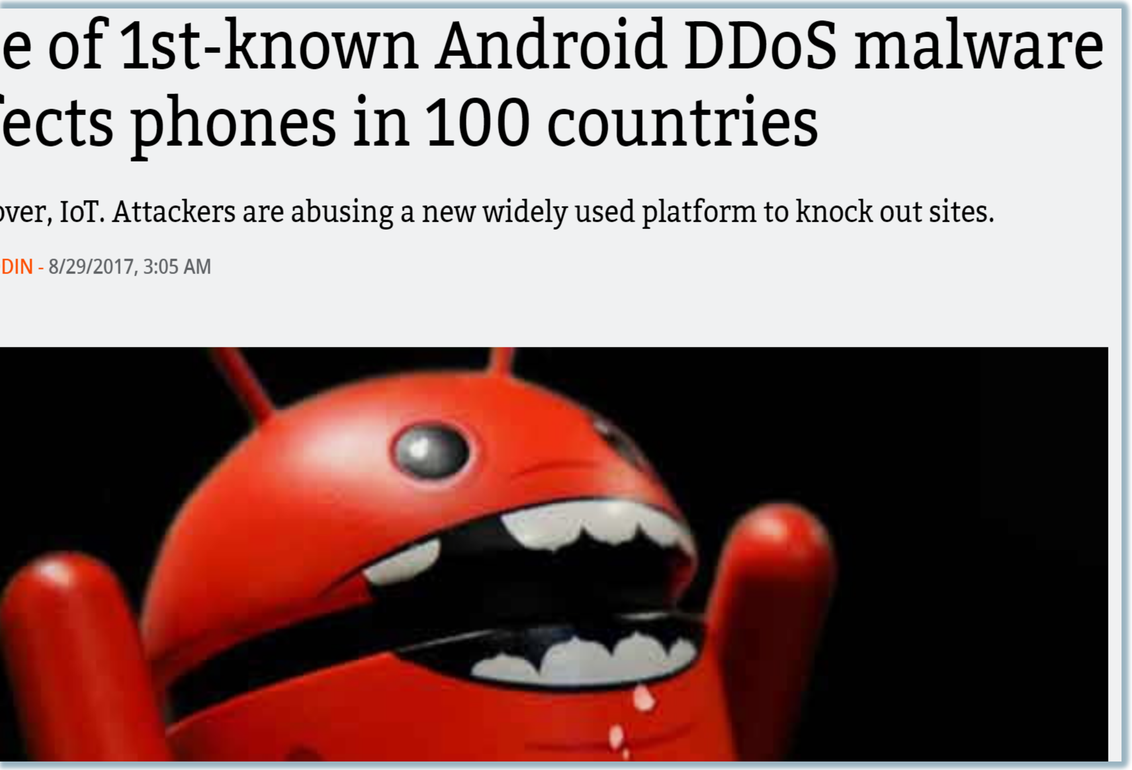
A map showing areas of Internet outages the morning of Friday, October 21, 2016. At the distributed denial of service attack on Dyn, an Internet and DNS service provider was un



ıfter quietly infecting a million devices, ɛeaper botnet set to be worse than Mirai

ıper is on track to become one of the largest botnets recorded in recent years — and yet nobody seems ·w what it will do or when. But researchers say the damage could be bigger than last year's cyberattack.

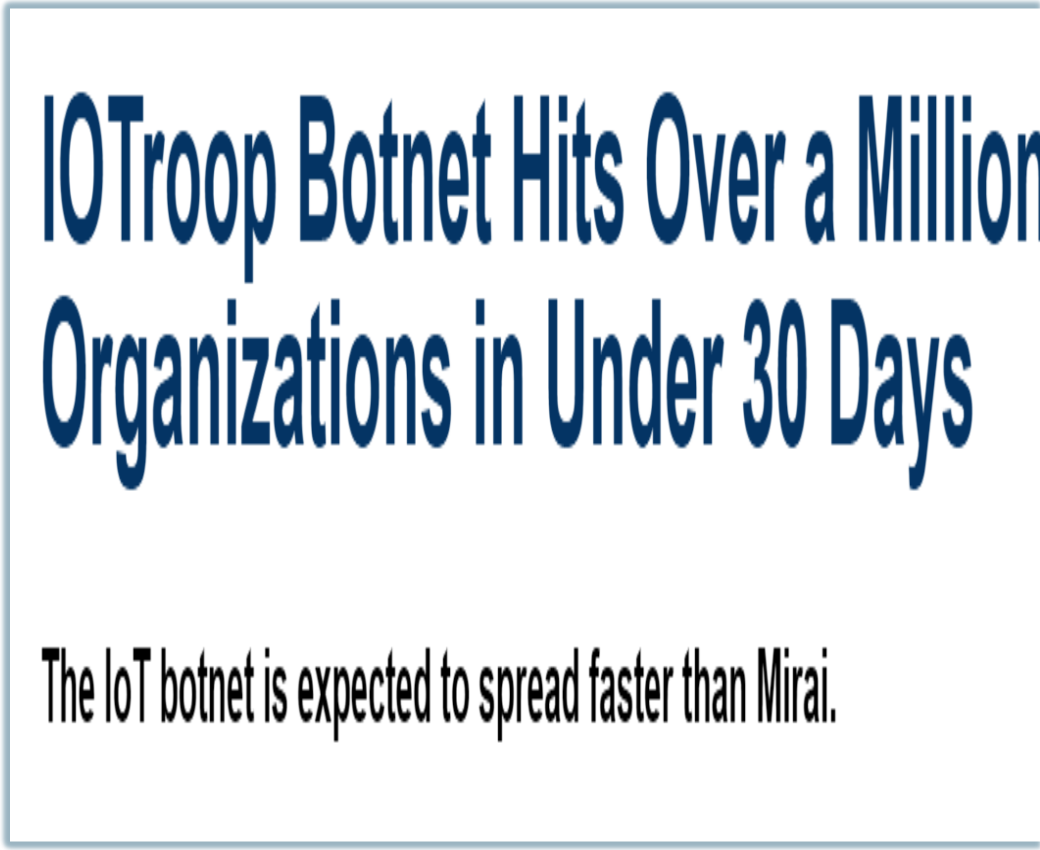
By Zack Whittaker for Zero Day | October 24, 2017 -- 12:46 GMT (05:46 PDT) | Topic: Security



e of 1st-known Android DDoS malware ̇ects phones in 100 countries

over, IoT. Attackers are abusing a new widely used platform to knock out sites.

DIN - 8/29/2017, 3:05 AM



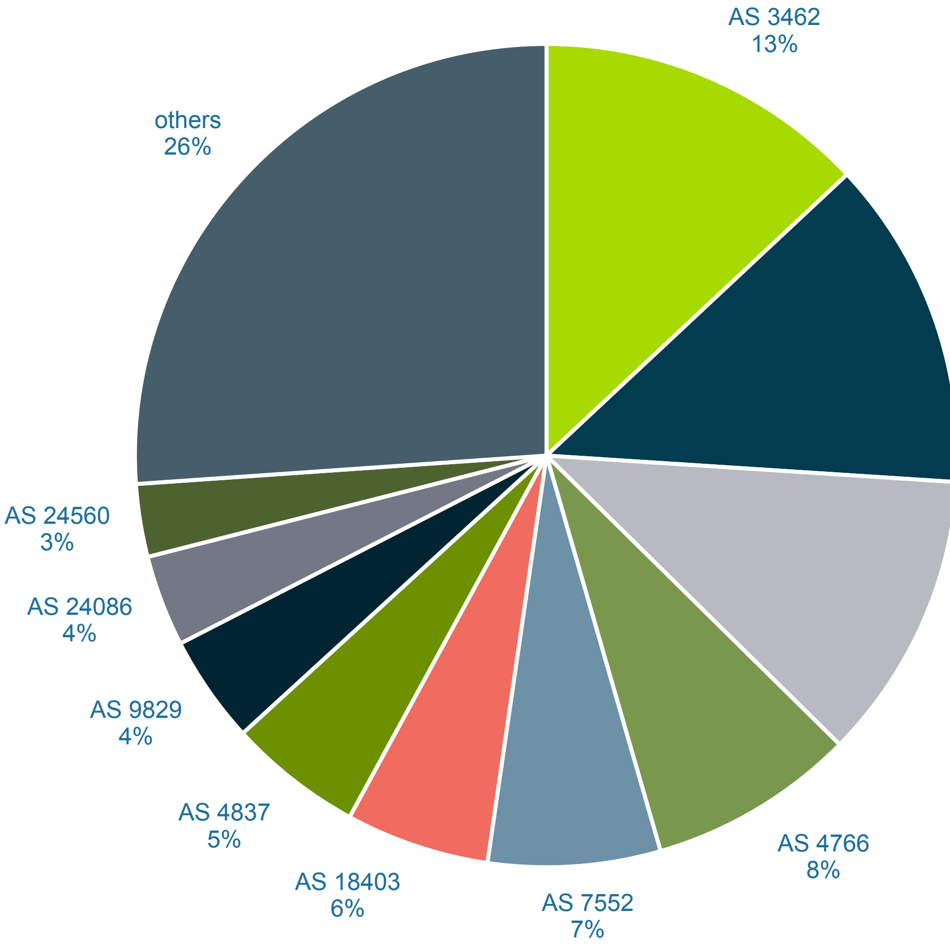
IOTroop Botnet Hits Over a Million Organizations in Under 30 Days

The IoT botnet is expected to spread faster than Mirai.

ATLAS IoT Botnet tracking

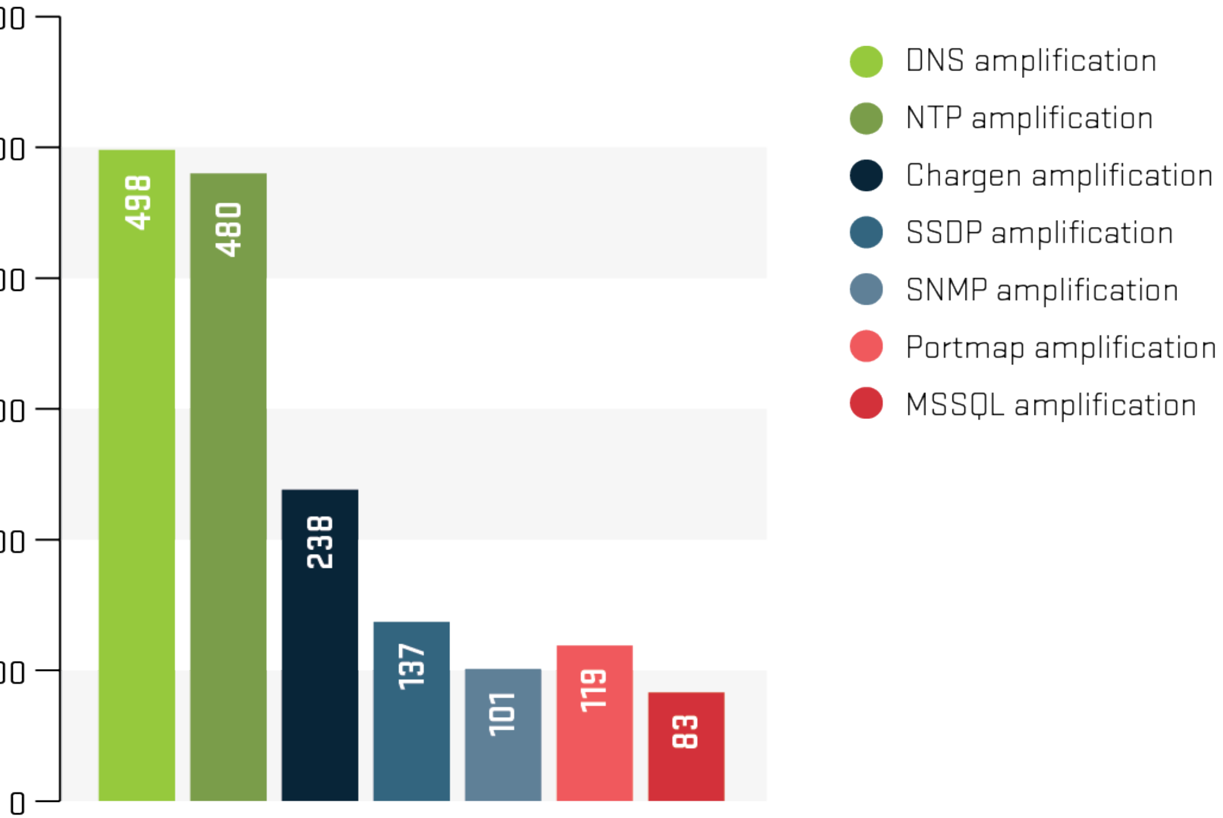
Country	Number of Attempts
China	102,975
Vietnam	26,573
Republic of Korea	19,465
USA	17,062
Brazil	16,609
Russia	13,378
Taiwan	11,697
Hong Kong	11,200
Turkey	10,190
Romania	9,856

Login attempts by APAC ASN



Scale: Driving Factors, Reflection Amplification

ATLAS Reflection/Amplification Attacks, Peak Sizes (Gbps)



Source: Arbor Networks, Inc.

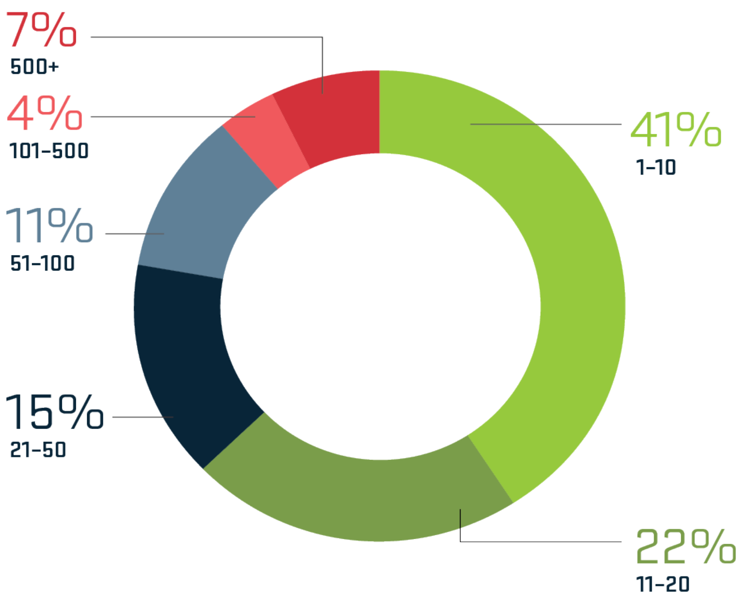
- Reflection Amplification attacks continue but there has been some cyclic change the protocols favored by attackers.
- Strong growth in the use of DNS (again) through 2016
- Largest monitored attack of 498.3Gbs, a 97% jump from last year
  - DNS and NTP attacks over 400Gbps, Chargen over 200Gbps

1 Every 6 Seconds

DDoS Attacks

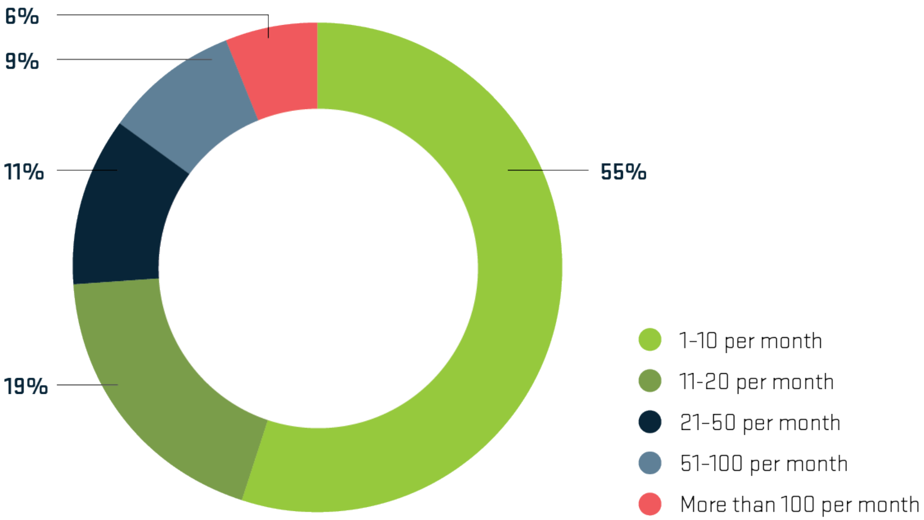
requency : Up Across the Board

Data Center DDoS Attack Frequency



Source: Arbor Networks, Inc.

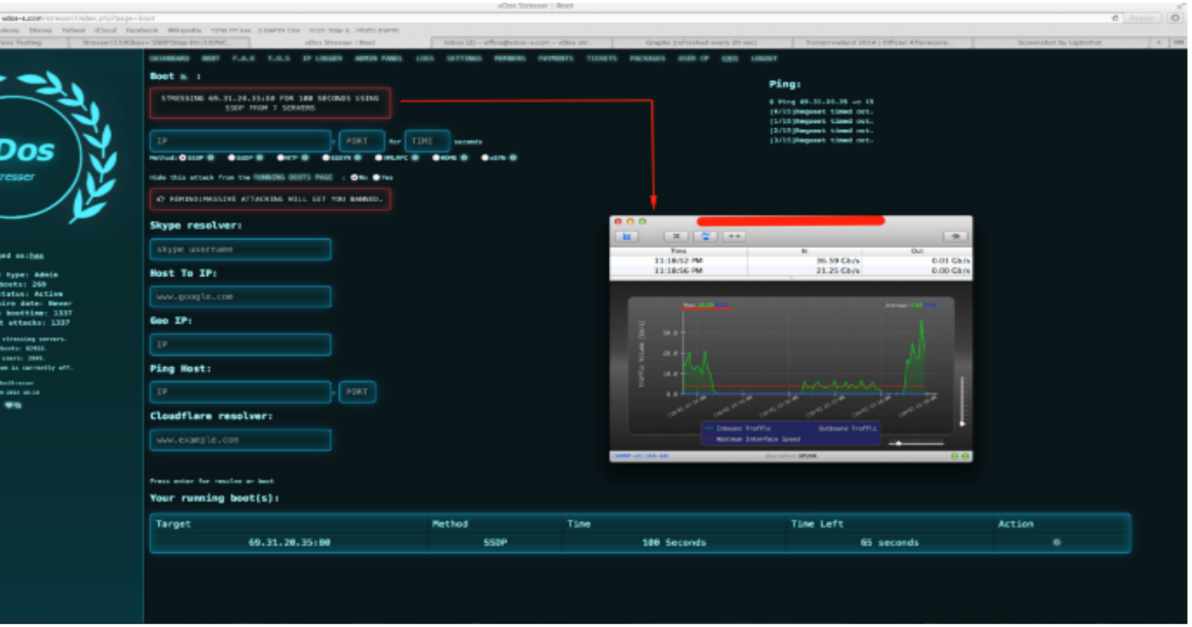
EGE DDoS Attack Frequency Per Month



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.

equency - Weaponization of DDoS


vDos Stresser | Boot
DASHBOARD BOOT F.A.Q T.O.S IP LOGGER ADMIN PANEL LOGS SETTINGS MEMBERS PAYMENTS TICKETS PACKAGES LOGOUT
Dos
resser

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: skype username

Host To IP: www.google.com

Geo IP: IP

Ping Host: IP : PORT

Cloudflare resolver: www.example.com

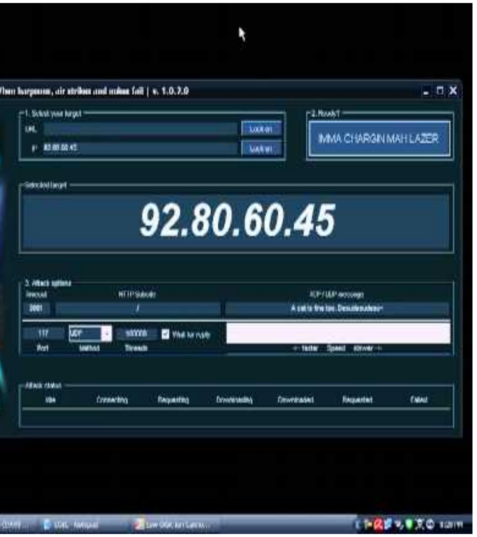
Press enter for resolve or boot

Your running boot(s):

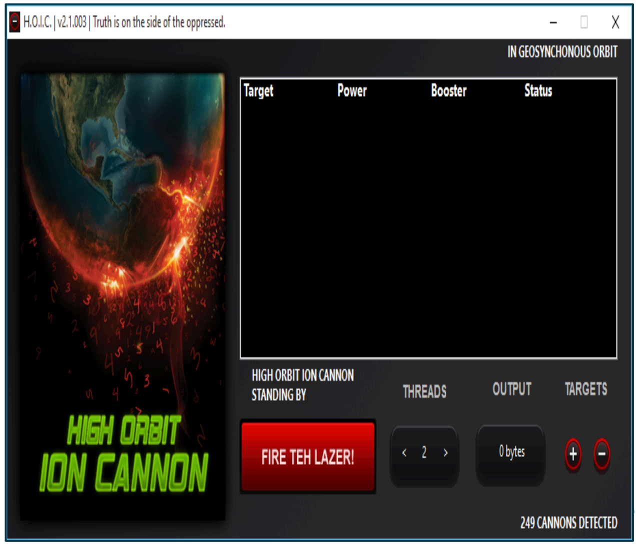
Target	Method	Time	Time Left	Action
69.31.20.35:80	SSDP	100 Seconds	65 seconds	

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

- Increased availability of “Stresser Tools”/”Booters” which perform highly distributed attacks using a combination of non-spoofed and spoofed amplification attacks. Often linked to bot-farms.

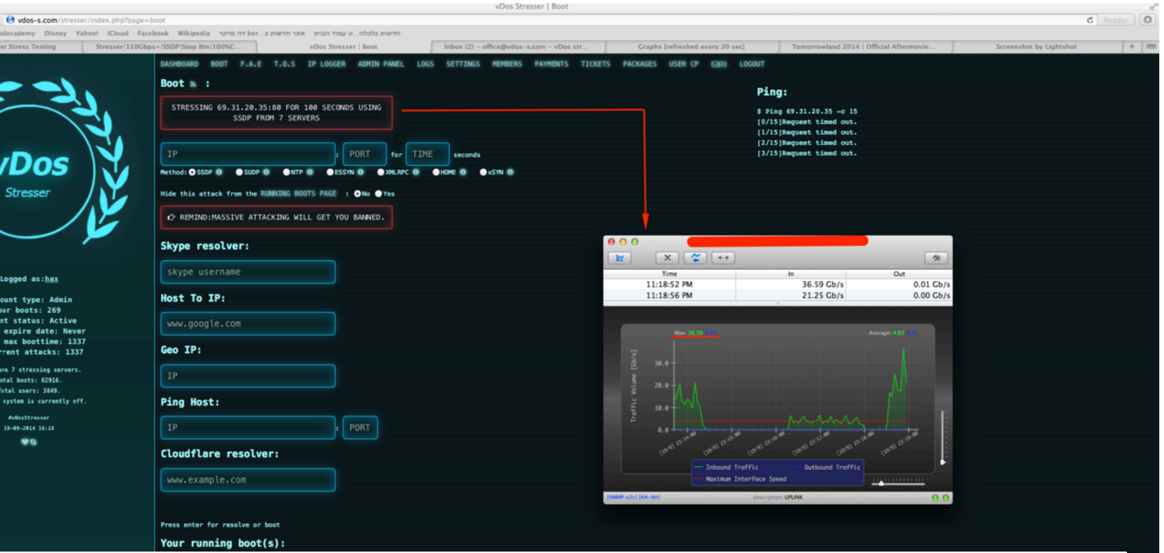


92.80.60.45



- Development of tools for use by voluntarily opt-in attackers:
  - Low Orbit Ion Cannon used to perform non-spoofed UDP/ICMP attacks
  - High Orbit Ion Cannon sends non-spoofed HTTP requests against multiple sites

Frequency - DDoS tools for the masses



vDos Stresser | Boot
vdos-s.com/stresser/index.php?page=boot
DASHBOARD BOOT F.A.E T.O.S IP LOGGER ADMIN PANEL LOGS SETTINGS MEMBERS PAYMENTS TICKETS PACKAGES USER CP (0) LOGOUT
vDos Stresser

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):

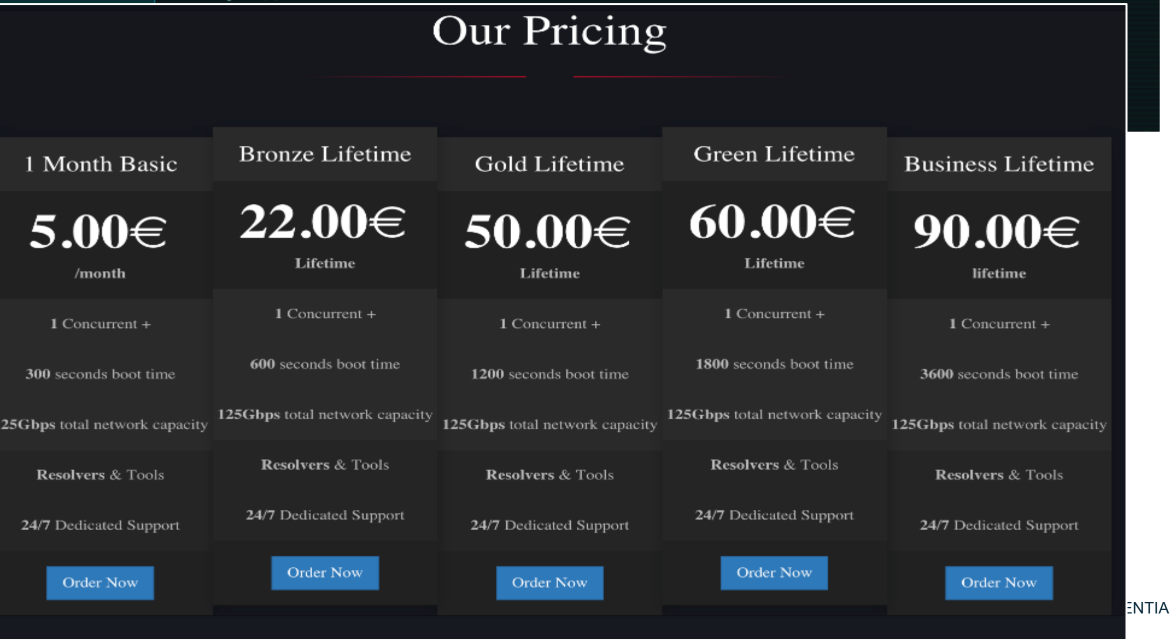
```
Logged as:hax
count type: Admin
our boots: 269
nt status: Active
 expire date: Never
 max boottime: 1337
rrent attacks: 1337
are 7 stressing servers.
otal boots: 82916.
Total users: 3849.
 system is currently off.
#vDosStresser
19-09-2014 16:18
```

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

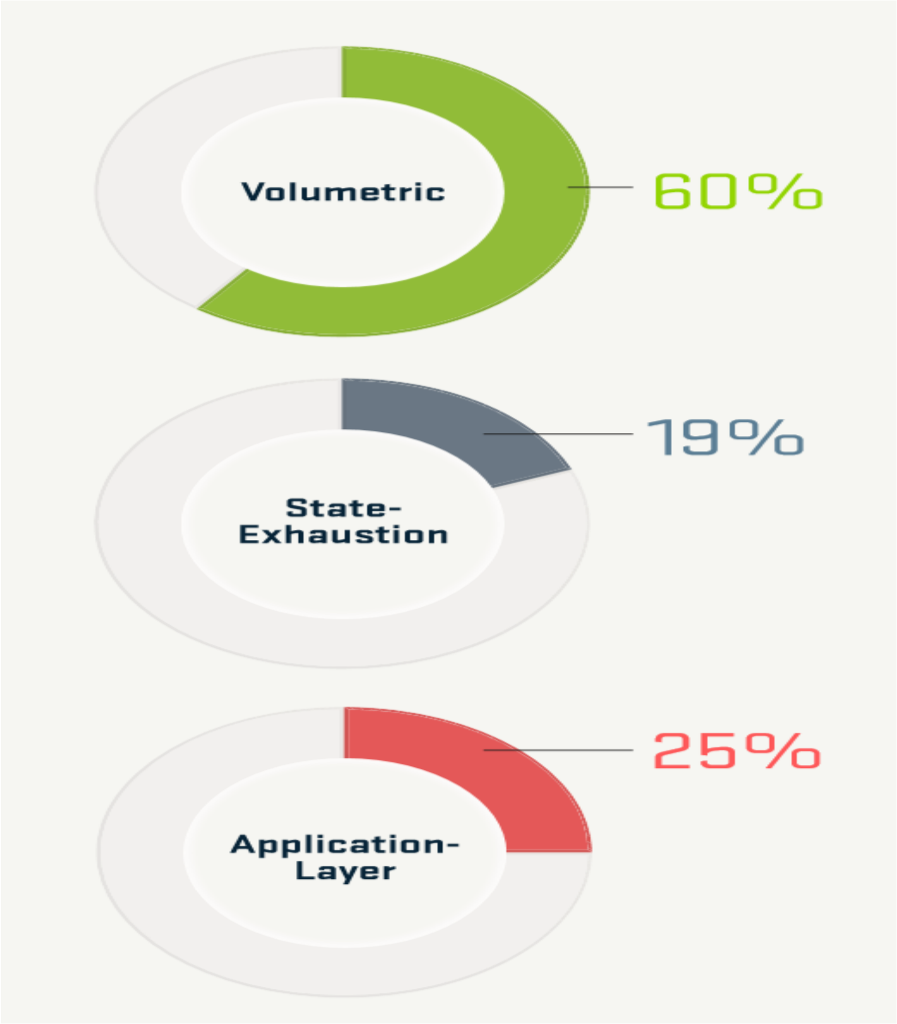


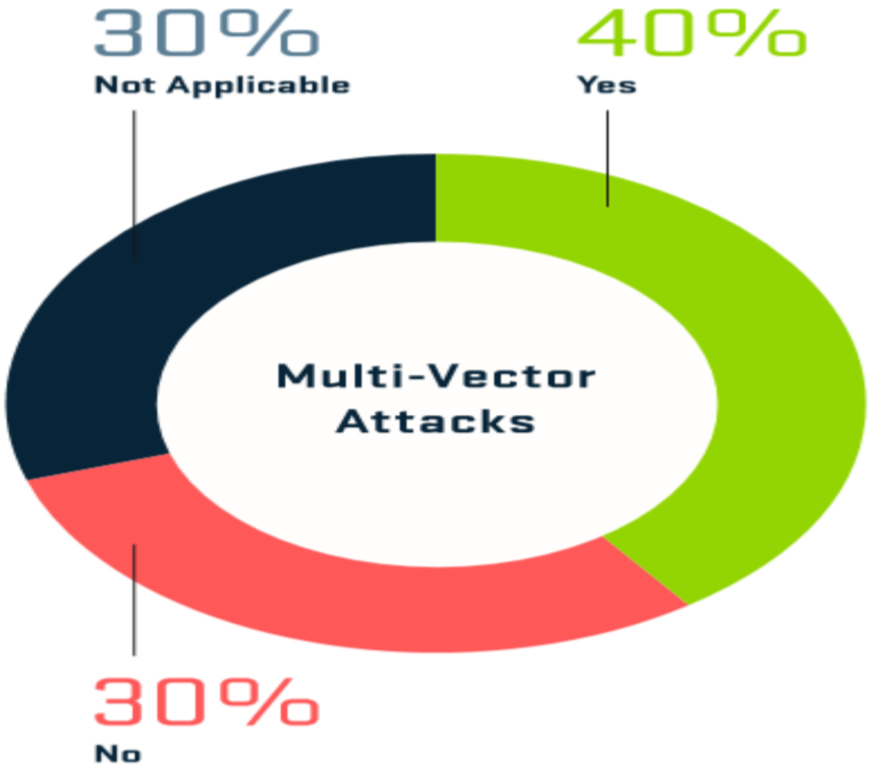
Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
5.00€ /month	22.00€ Lifetime	50.00€ Lifetime	60.00€ Lifetime	90.00€ 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
25Gbps 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

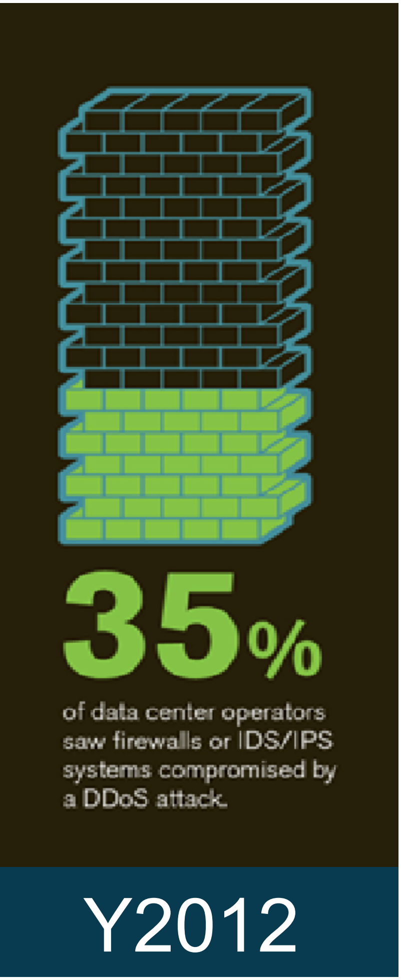
- Anyone which has the capability to click a button can now launch an DDoS attack.
- Cheap and simple to use:
  - VIP accounts!
  - Lifetime subscription!
  - 24x7 customer support!
- Primarily used by gamers attacking each other but recently we have bee seeing them used to attack highly visible targets.

omplexity : EGE Attack Types





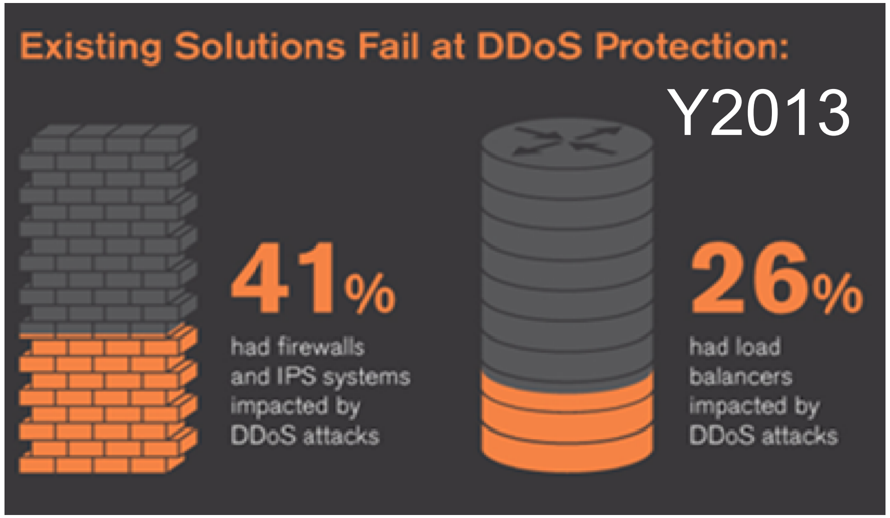
REWALL, IPS, LOAD BALANCER FAIL TO STOP DDOS TTACKS



35%

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

Y2012

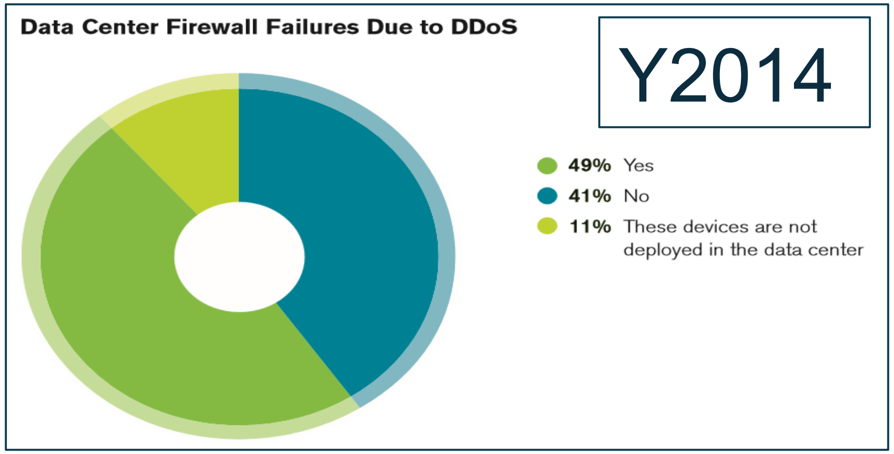


Existing Solutions Fail at DDoS Protection:

Y2013

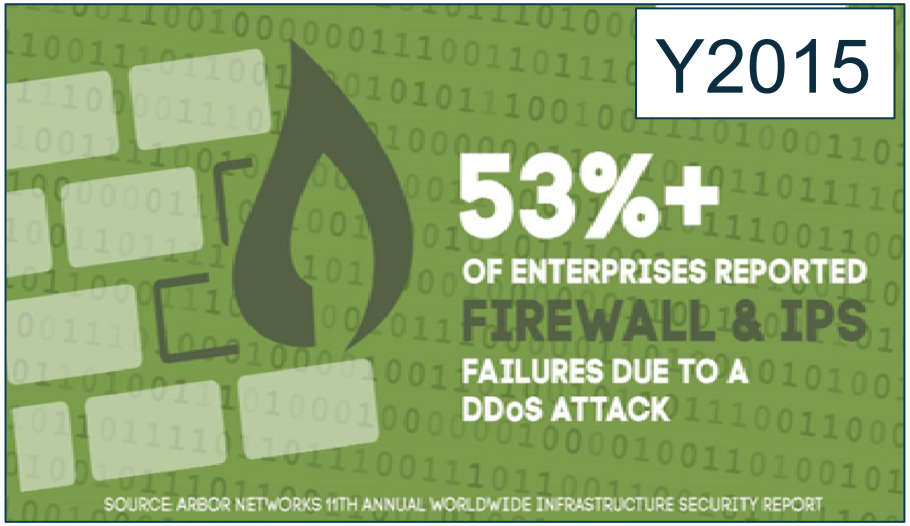
41% had firewalls and IPS systems impacted by DDoS attacks

26% had load balancers impacted by DDoS attacks



Data Center Firewall Failures Due to DDoS

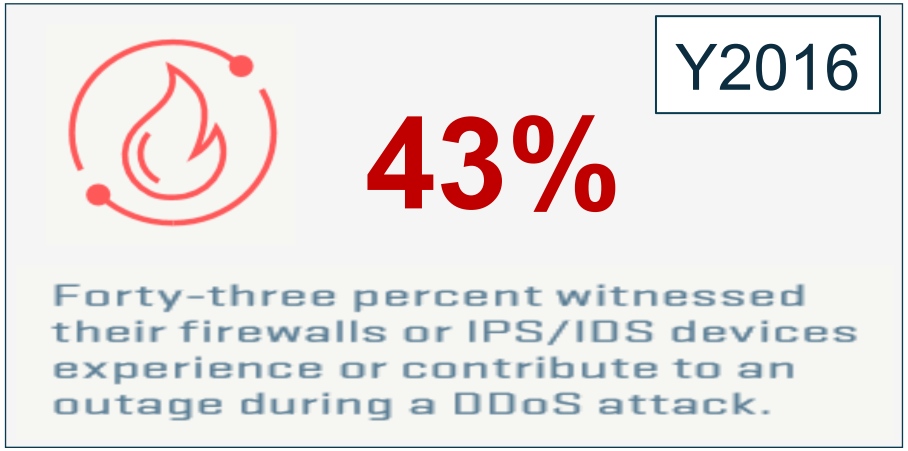
Y2014



Y2015

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

SOURCE: ARBOR NETWORKS 11TH ANNUAL WORLDWIDE INFRASTRUCTURE SECURITY REPORT



Y2016

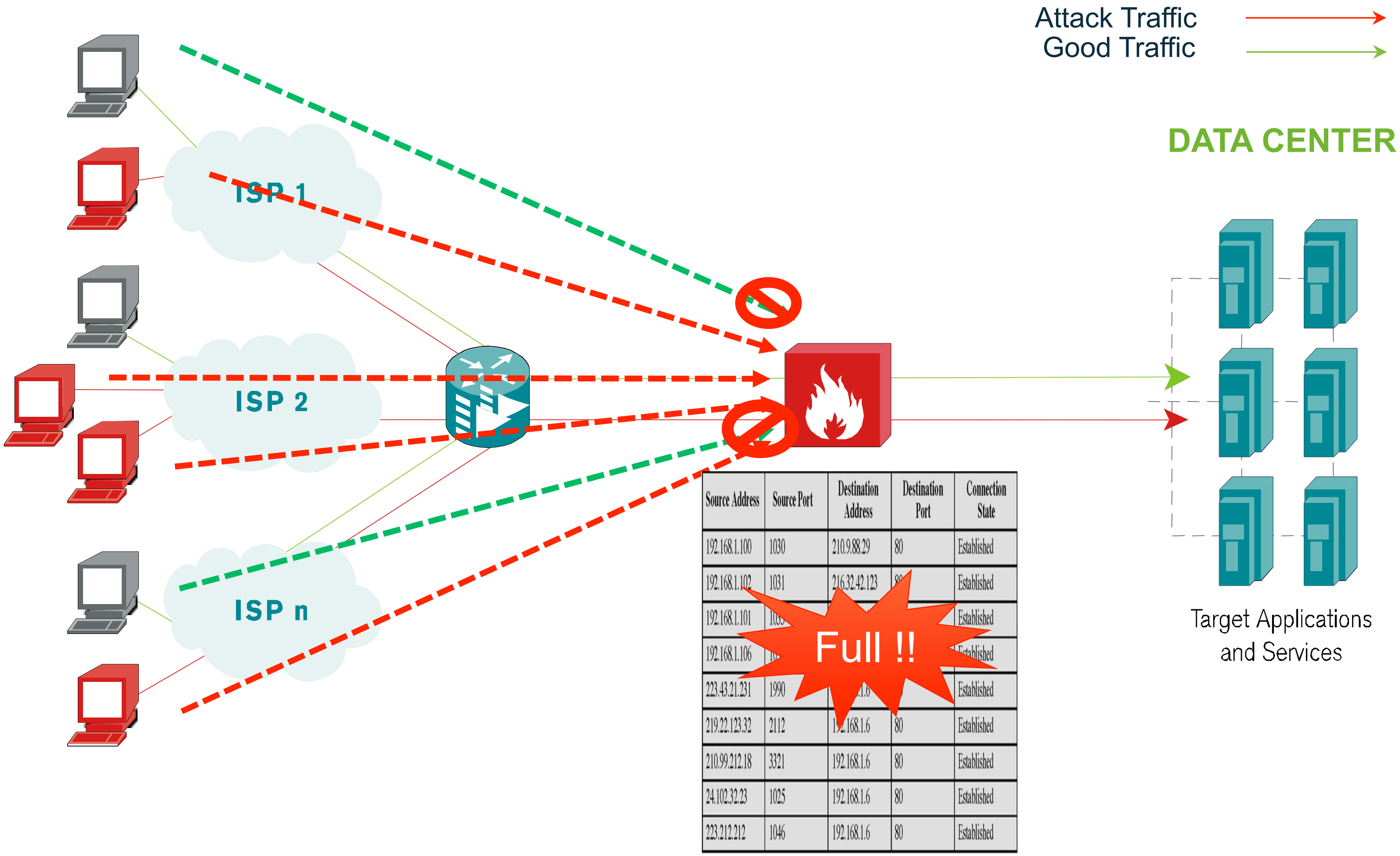
43%

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

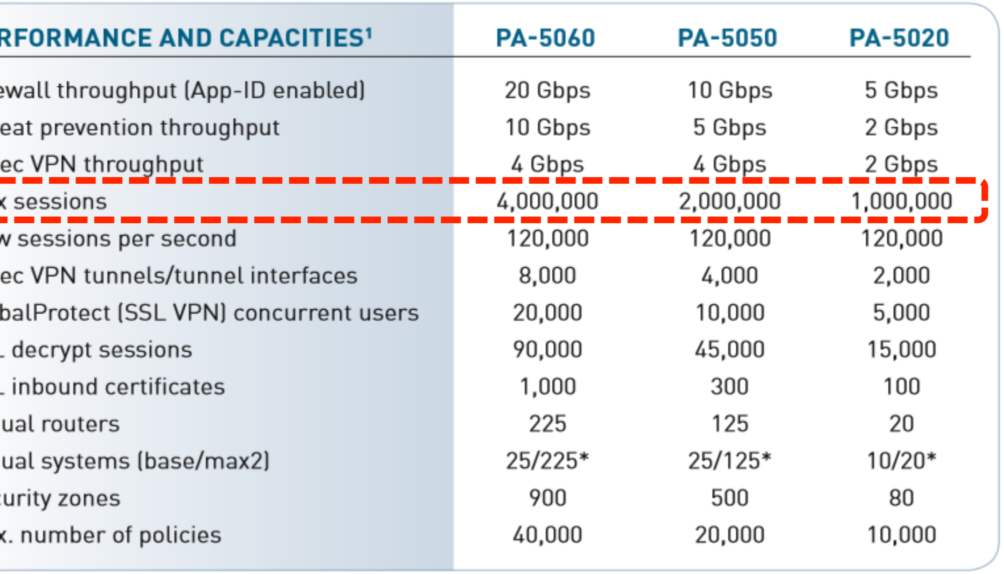
ARBOR® NETWORKS

TATE EXHAUSTION DDOS ATTACK

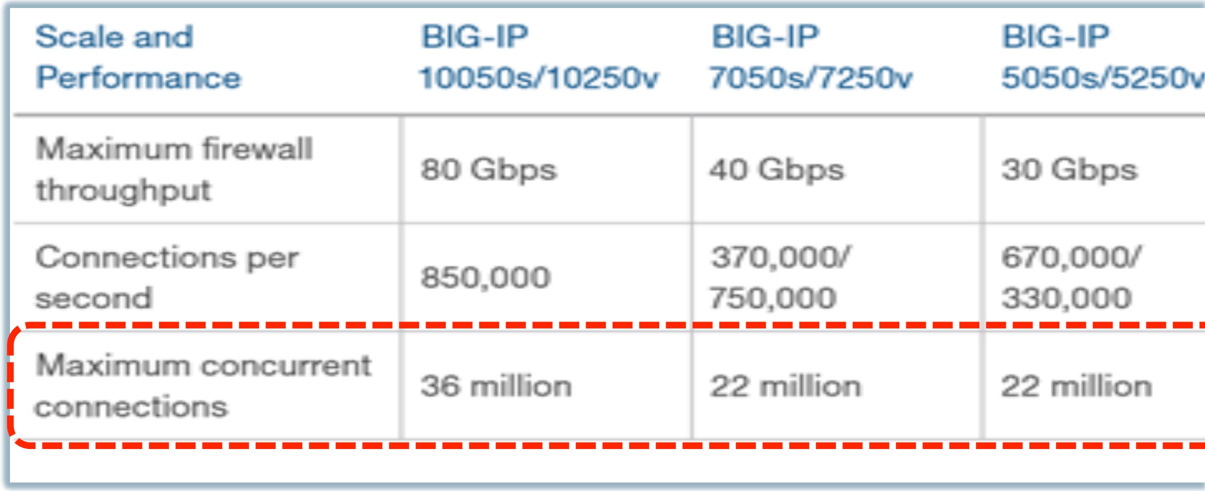


Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	[illegible]	[illegible]	[illegible]	Established
192.168.1.106	[illegible]	[illegible]	[illegible]	Established
223.43.21.231	1990	[illegible]	[illegible]	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.212.212	1046	192.168.1.6	80	Established

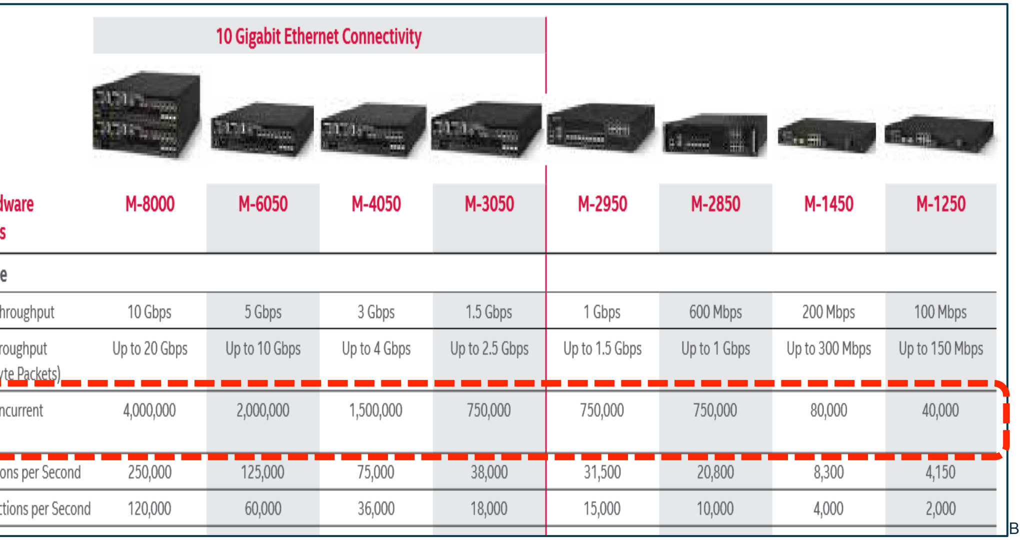
TATEFUL DEVICE ?



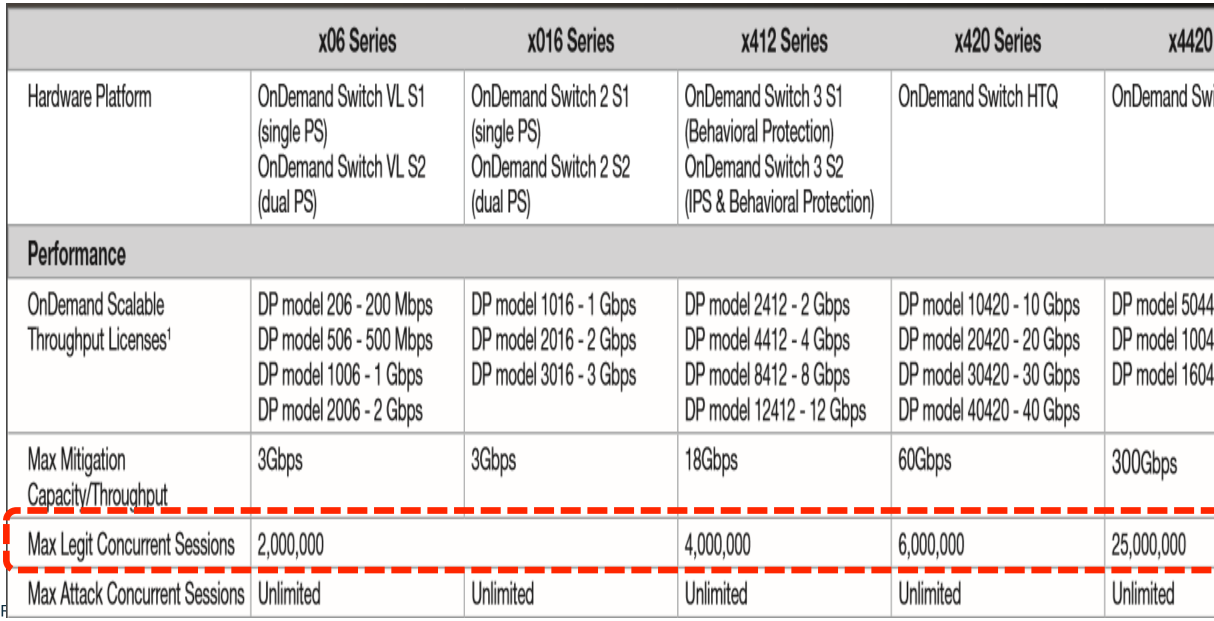
RFORMANCE AND CAPACITIES[1]	PA-5060	PA-5050	PA-5020
ewall throughput (App-ID enabled)	20 Gbps	10 Gbps	5 Gbps
eat prevention throughput	10 Gbps	5 Gbps	2 Gbps
ec VPN throughput	4 Gbps	4 Gbps	2 Gbps
x sessions	4,000,000	2,000,000	1,000,000
w sessions per second	120,000	120,000	120,000
ec VPN tunnels/tunnel interfaces	8,000	4,000	2,000
balProtect (SSL VPN) concurrent users	20,000	10,000	5,000
. decrypt sessions	90,000	45,000	15,000
. inbound certificates	1,000	300	100
ual routers	225	125	20
ual systems (base/max2)	25/225*	25/125*	10/20*
urity zones	900	500	80
x. number of policies	40,000	20,000	10,000



Scale and Performance	BIG-IP 10050s/10250v	BIG-IP 7050s/7250v	BIG-IP 5050s/5250v
Maximum firewall throughput	80 Gbps	40 Gbps	30 Gbps
Connections per second	850,000	370,000/ 750,000	670,000/ 330,000
Maximum concurrent connections	36 million	22 million	22 million



	10 Gigabit Ethernet Connectivity							
dware s	M-8000	M-6050	M-4050	M-3050	M-2950	M-2850	M-1450	M-1250
e								
hroughput	10 Gbps	5 Gbps	3 Gbps	1.5 Gbps	1 Gbps	600 Mbps	200 Mbps	100 Mbps
roughput yte Packets)	Up to 20 Gbps	Up to 10 Gbps	Up to 4 Gbps	Up to 2.5 Gbps	Up to 1.5 Gbps	Up to 1 Gbps	Up to 300 Mbps	Up to 150 Mbps
ncurrent	4,000,000	2,000,000	1,500,000	750,000	750,000	750,000	80,000	40,000
ons per Second	250,000	125,000	75,000	38,000	31,500	20,800	8,300	4,150
ctions per Second	120,000	60,000	36,000	18,000	15,000	10,000	4,000	2,000



	x06 Series	x016 Series	x412 Series	x420 Series	x4420
Hardware Platform	OnDemand Switch VL S1 (single PS) OnDemand Switch VL S2 (dual PS)	OnDemand Switch 2 S1 (single PS) OnDemand Switch 2 S2 (dual PS)	OnDemand Switch 3 S1 (Behavioral Protection) OnDemand Switch 3 S2 (IPS & Behavioral Protection)	OnDemand Switch HTQ	OnDemand Swi
Performance					
OnDemand Scalable Throughput Licenses[1]	DP model 206 - 200 Mbps DP model 506 - 500 Mbps DP model 1006 - 1 Gbps DP model 2006 - 2 Gbps	DP model 1016 - 1 Gbps DP model 2016 - 2 Gbps DP model 3016 - 3 Gbps	DP model 2412 - 2 Gbps DP model 4412 - 4 Gbps DP model 8412 - 8 Gbps DP model 12412 - 12 Gbps	DP model 10420 - 10 Gbps DP model 20420 - 20 Gbps DP model 30420 - 30 Gbps DP model 40420 - 40 Gbps	DP model 5044 DP model 1004 DP model 1604
Max Mitigation Capacity/Throughput	3Gbps	3Gbps	18Gbps	60Gbps	300Gbps
Max Legit Concurrent Sessions	2,000,000		4,000,000	6,000,000	25,000,000
Max Attack Concurrent Sessions	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

DDoS Targets

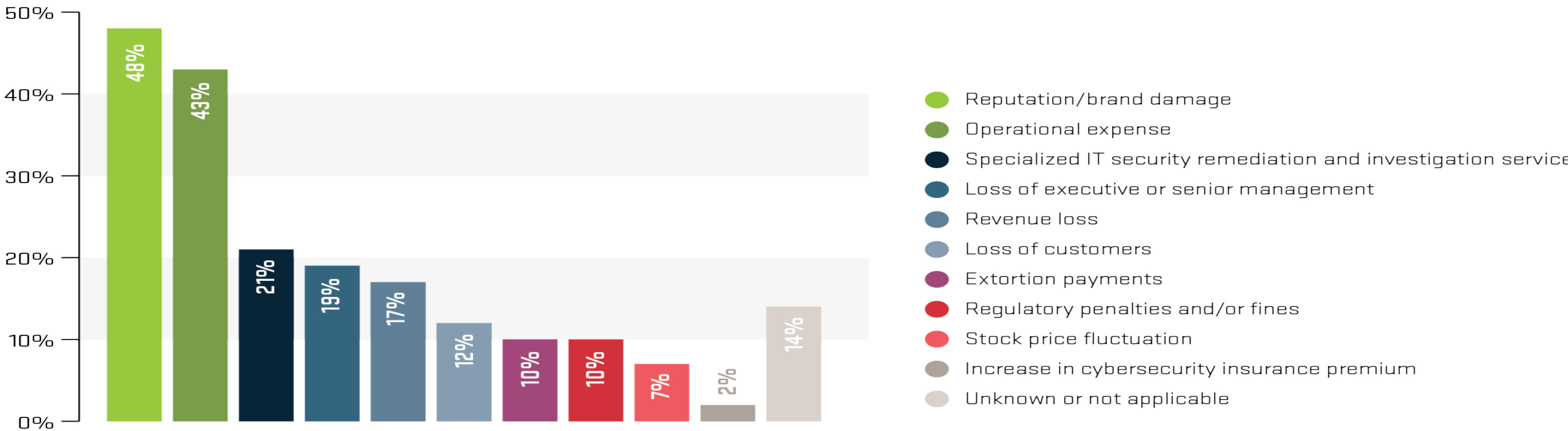
Attack Target Customer Verticals

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.

npact : Enterprise

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

Thank You

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

ARBOR NETWORKS
The Security Division of NETSCOUT