DDoS Threat Landscape

Challenges faced by Network Operators

ARBOR® NETWORKS

WISR 2016 Survey Highlights

- The Arbor Networks' eleventh annual Worldwide Infrastructure Security Report (WISR) is released in Jan.
- Largest reported attack jumps to 500Gbps
  - Over 60X increase from 8Gbps eleven years ago!
- Application-layer attacks monitored by nearly all service providers
  - 56 percent saw multi-vector attacks, up from 42 percent last year.
- Existing infrastructure, such as firewall and IPS devices, continue to be targeted by DDoS attacks
  - Over half of enterprises report these devices failing as a result of a DDoS attack - up significantly from one third last year
- Data center operators continue to struggle with the rise in volumetric attacks
  - Over half of data center operators saw DDoS attacks which exhausted their Internet bandwidth - up from 33 percent last year
- An increasing number of service provider respondents are experiencing bandwidth saturation due to streaming, OTT, unique events, etc.
- The most common service targeted by application-layer attacks is now, for the first time, DNS.

SURVEY DEMOGRAPHICS

Respondent's Role in Organization

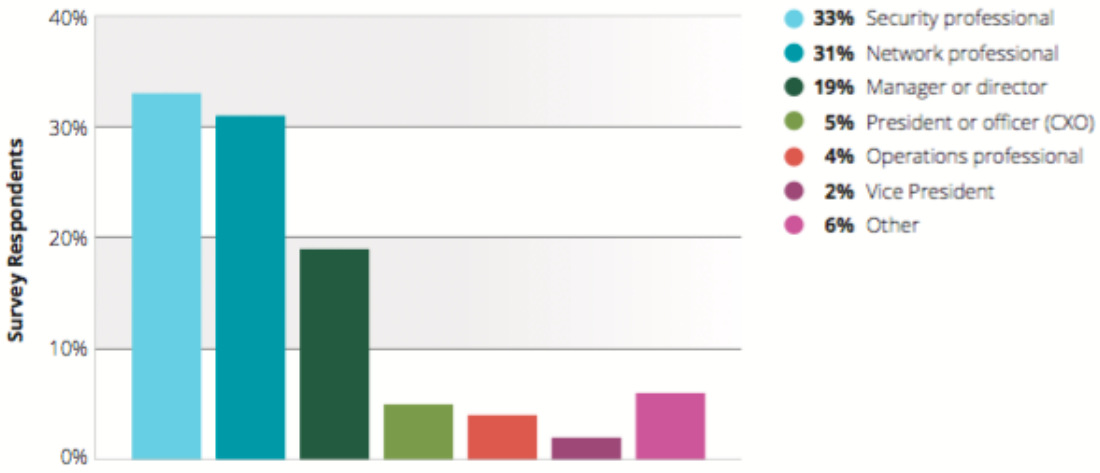
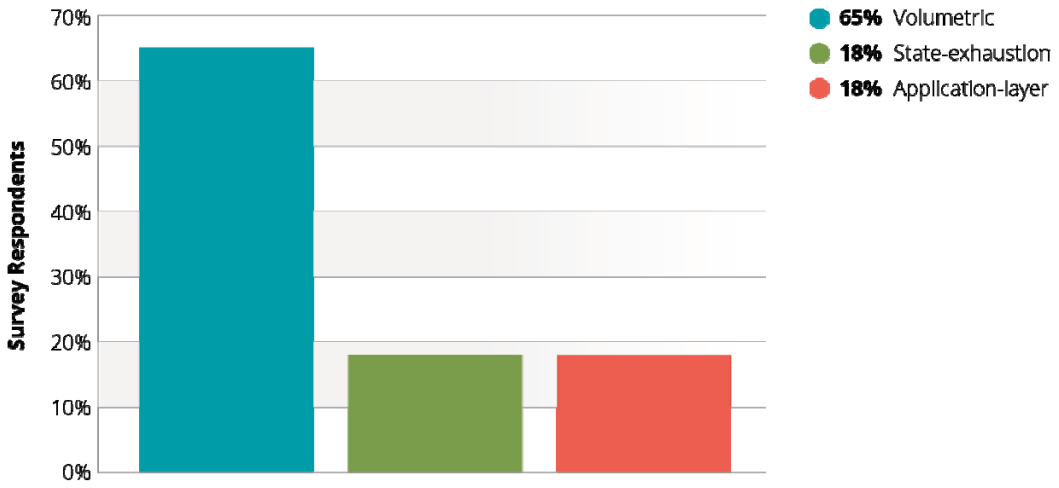


Figure 3 Source: Arbor Networks, Inc.

- Respondents represent 354 network operators from around the world - up from 287 last year
- Nearly half represent Enterprise, Government, and Education (EGE)
- United States and Canada lead regional participation, Europe a close second
- APAC, LATAM, Middle East and Africa about one-third

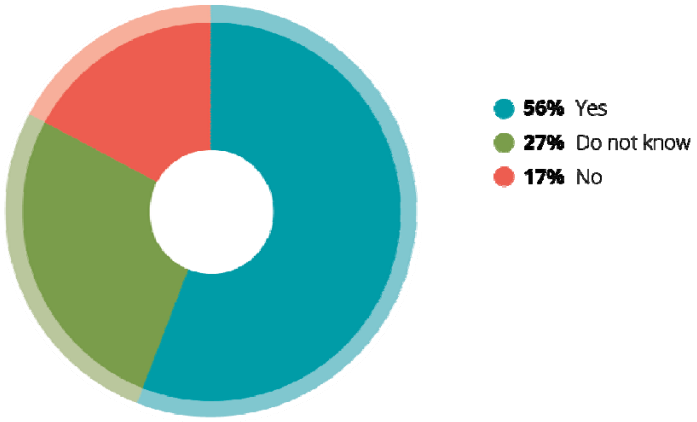
DDoS – Complexity Increases

DDoS Attack Types



Source: Arbor Networks, Inc.

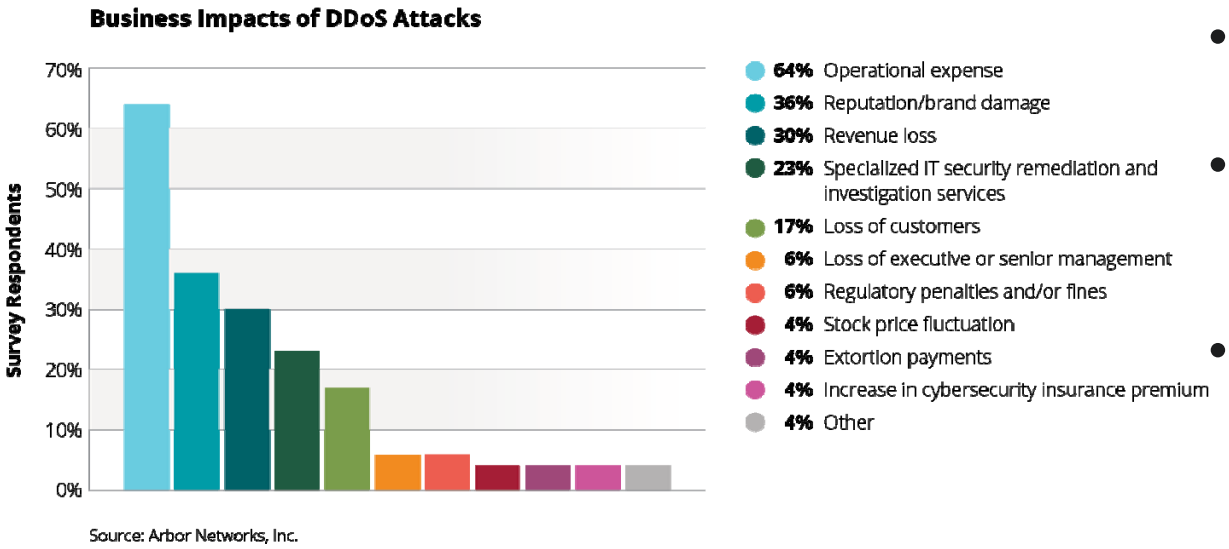
Multi-Vector DDoS Attacks



Source: Arbor Networks, Inc.

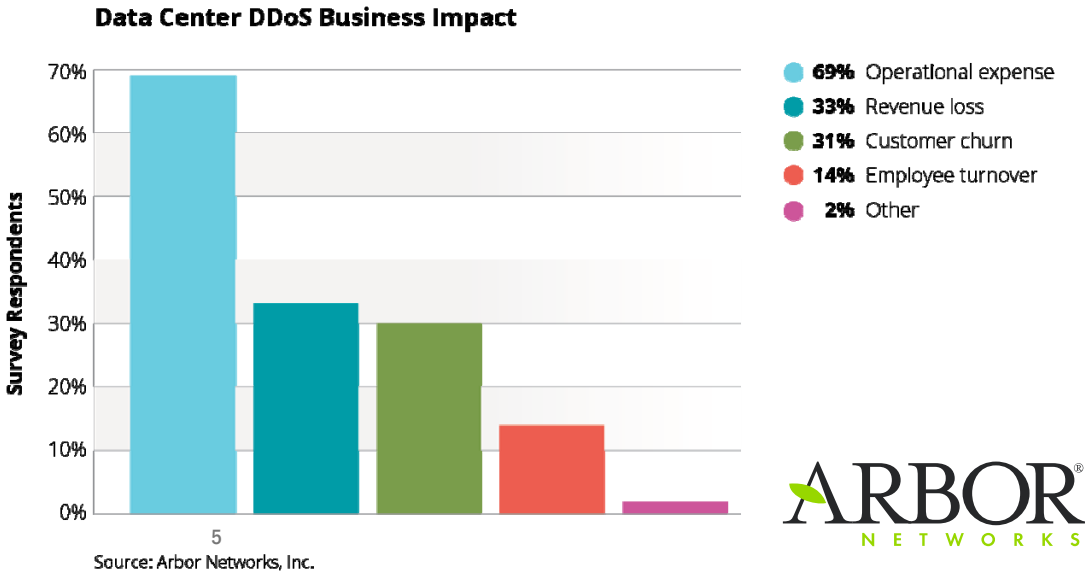
- Media focuses volumetric attacks but more stealthy application-layer attacks haven't gone away
  - 93% of respondents see application layer attacks, up from 90 percent last year and 86 percent in 2013.
- DNS is now top application layer target, over-taking HTTP
  - Strong growth in respondents seeing attacks targeting SIP / VoIP services, up from 9% to 19%
- Significant increase in multi-vector attacks, up to 56 percent from 42 percent last year

DDoS - Business Impact

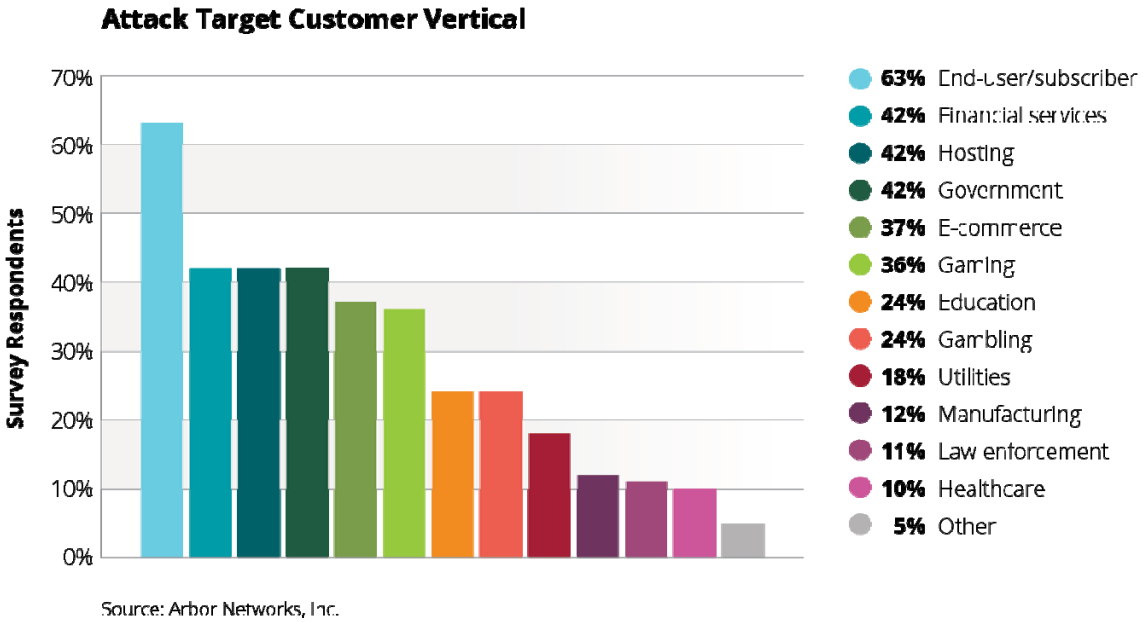


- Operational expenses top business impact
- 1/3 of Data Centers operators see revenue loss
- 36% of EGE see reputation / brand damage.

- Over half had Firewall/IPS device fail or contribute to outage during a DDoS attack



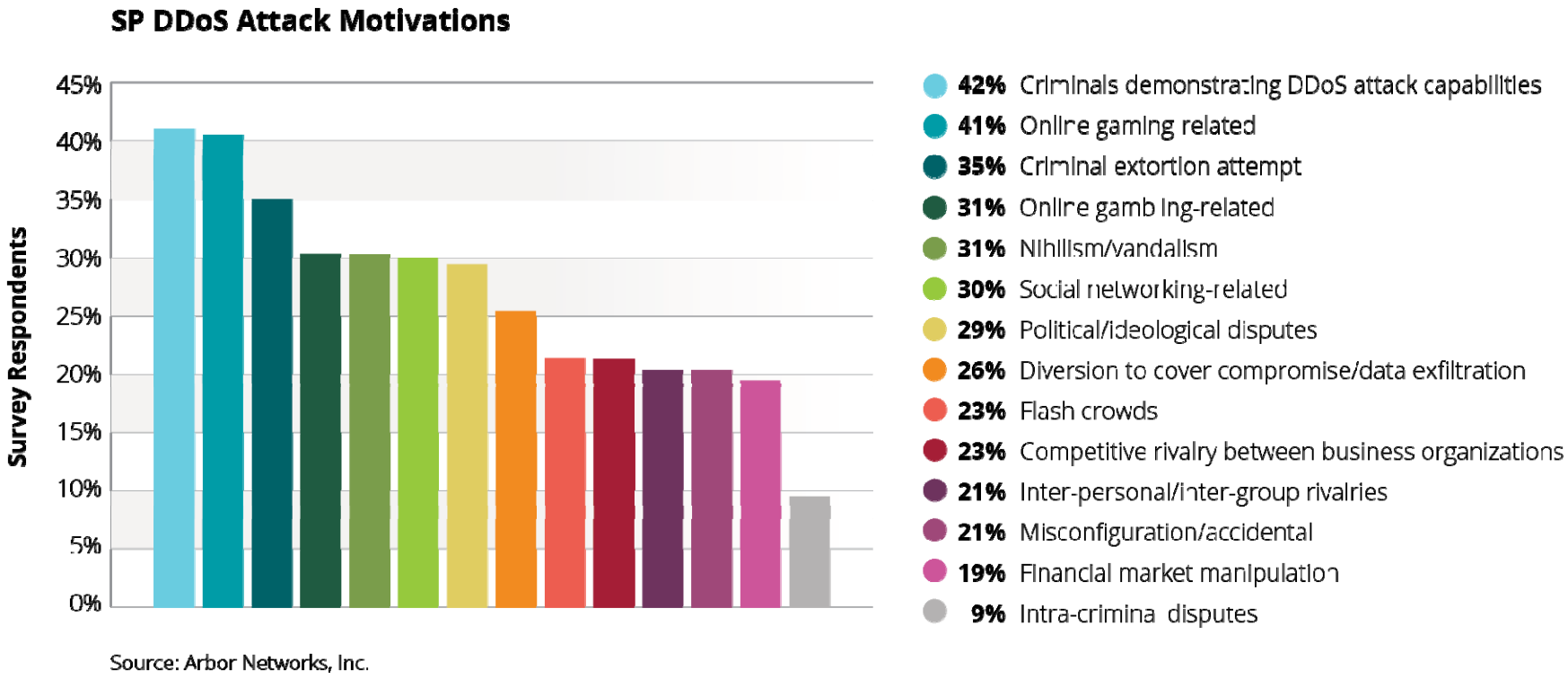
DDoS - Targets



Source: Arbor Networks, Inc.

- Service providers see their customers as the top target for DDoS attacks.
- Finance, government and hosting are the top targeted business verticals.
  - E-commerce moves down to third place.
- Continued growth in attacks targeting cloud services
  - 33% of respondents see attacks, up from 29% last year and 19% in 2013
- Big increase in proportion of respondents seeing attacks against IPv6 services
  - 9%, from 2% last year

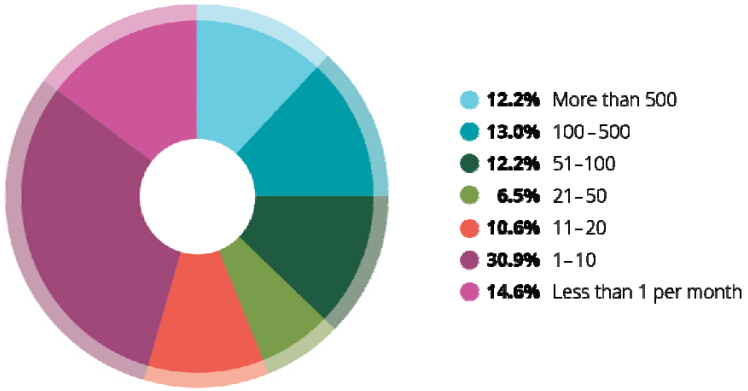
DDoS - Motivations



- Top perceived motivations include 'criminals demonstrating attack capabilities' and 'criminal extortion attempts'
- DDoS attacks being used as a distraction for either malware infiltration or data exfiltration on the rise

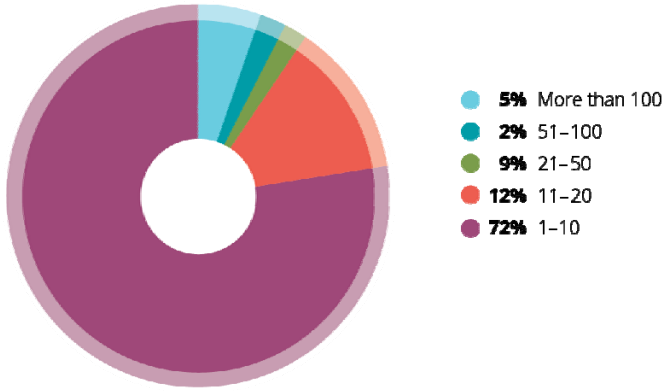
DDoS - Attack Frequency

SP DDoS Attack Frequency



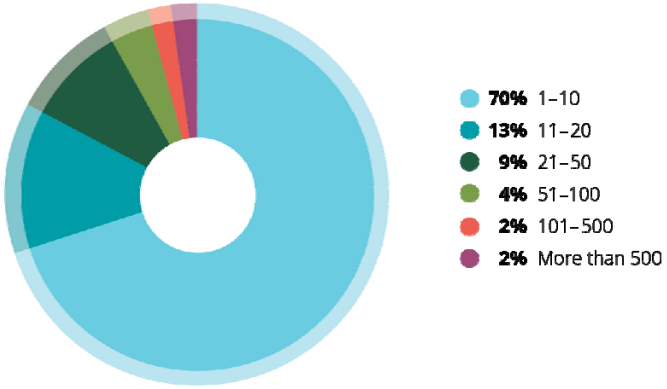
Source: Arbor Networks, Inc.

EGE DDoS Attack Frequency



Source: Arbor Networks, Inc.

Data Center DDoS Attack Frequency

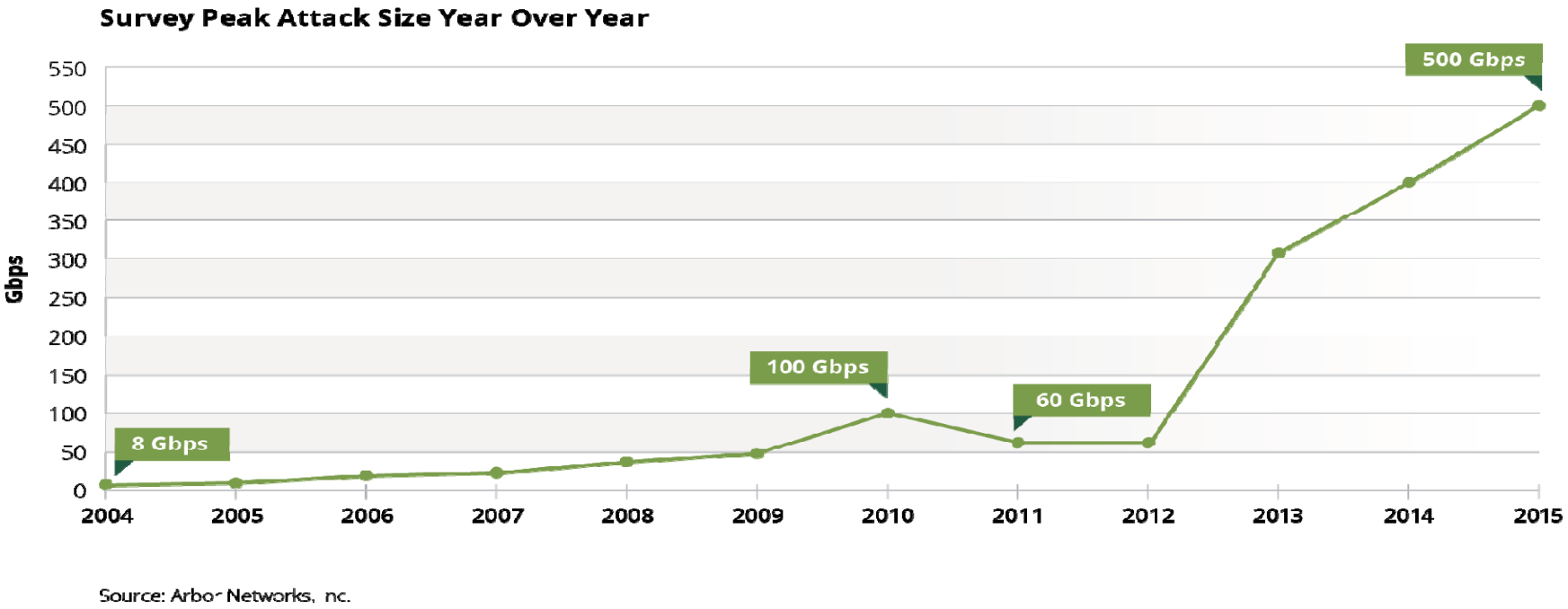


Source: Arbor Networks, Inc.

- 44% of service provider respondents have seen more than 21 attacks/month, up from 38% last year
- 28% of EGE respondents indicated they suffered more than 10 attacks per month
- 9% of data center operators seeing in > 50 attacks/month – none at this level last year

ARBOR NETWORKS

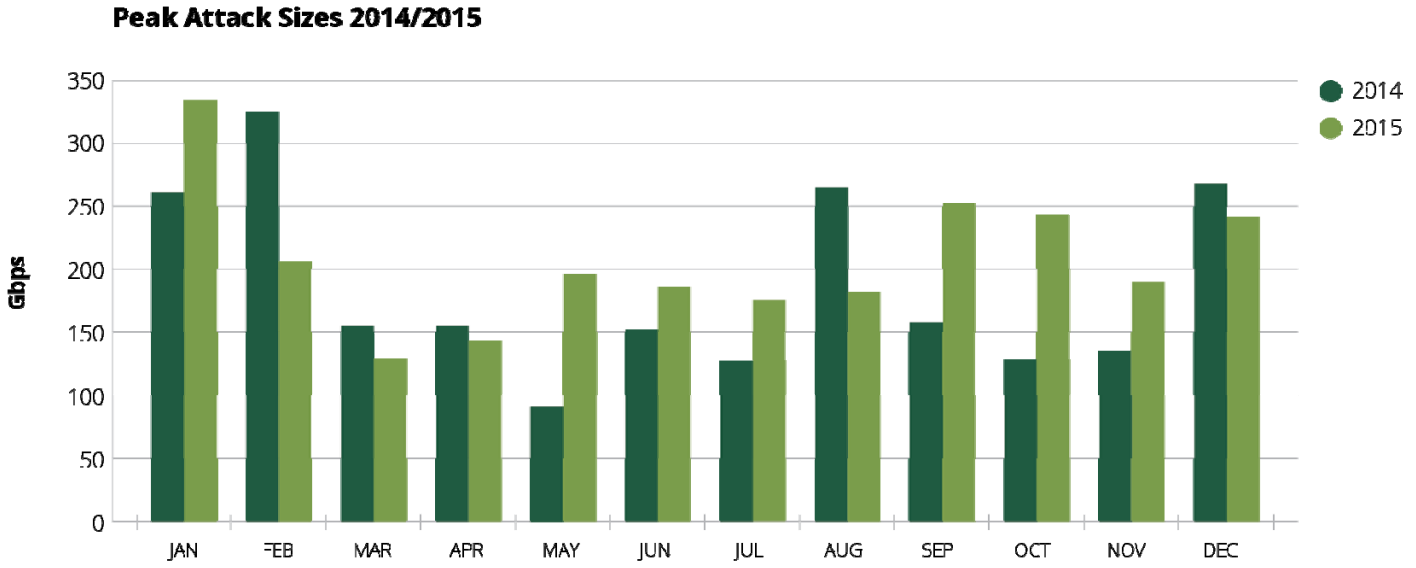
DDoS - Growth Continues



Source: Arbor Networks, Inc.

- Largest attack reported was 500 Gbps with other respondents reporting attacks of 450 Gbps, 425 Gbps, and 337 Gbps.
- Another five respondents reported 200+ Gbps attacks.
- Nearly one quarter of respondents reports peak attacks over 100Gbps
- Over half of EGE and Data-Centre respondents (respectively) saw attacks that completely saturated their Internet connectivity

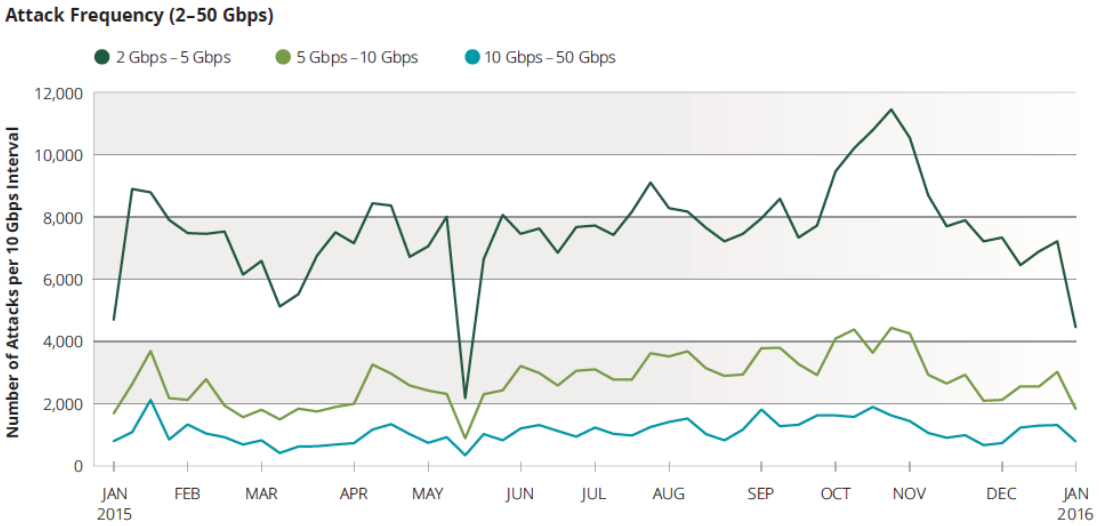
DDoS Growth, ATLAS Perspective

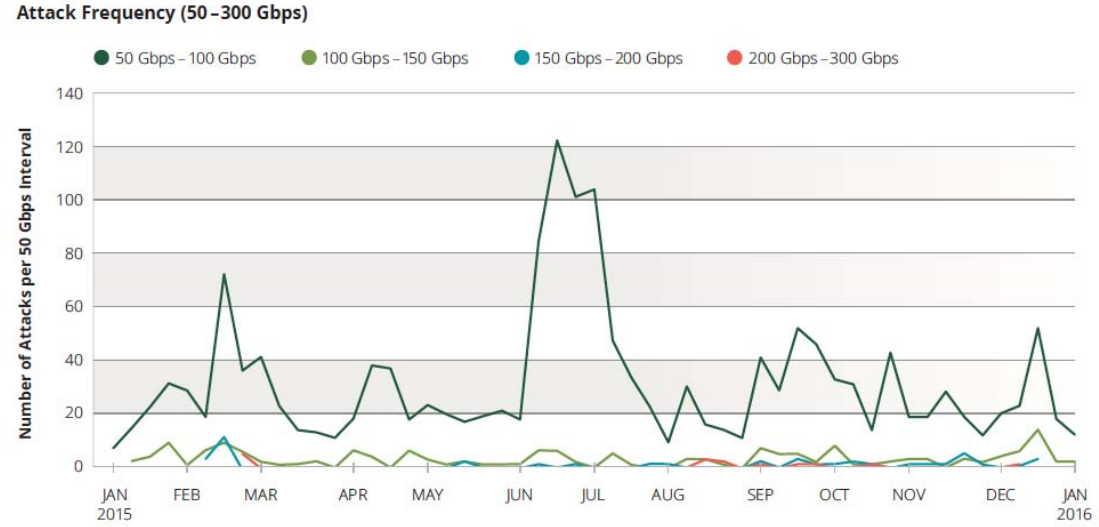


Source: Arbor Networks, Inc.

- Peak monitored, verified attack at 334Gbps
- 223 attacks over 100Gbps monitored, 16 of those over 200Gbps
  - 2013 saw 39 attacks over 100Gbps, 159 seen in 2014
- Upward trend in 2-50 Gbps attack frequency throughout 2015
- However, 84% of events still less than 1Gbps in size

Attack Frequency, ATLAS Perspective





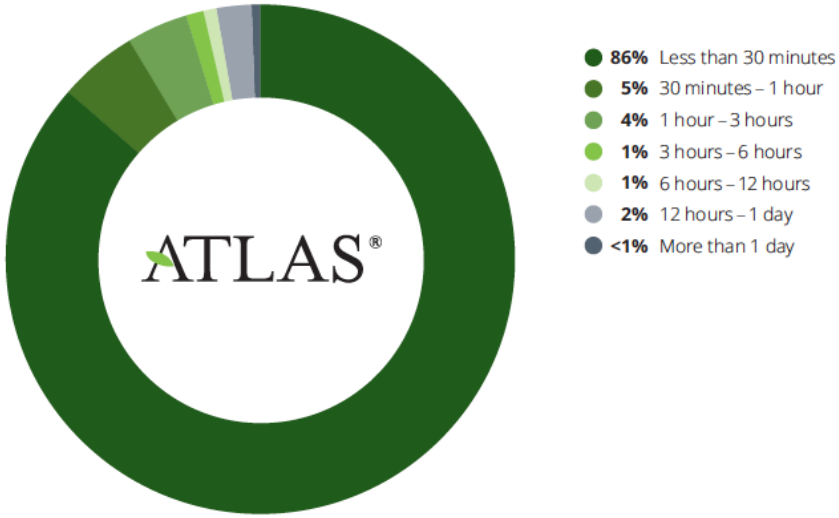
- Upward trend in frequency for 2-50 Gbps throughout the year
- No specific pattern/trend for larger attacks, probably related to specific attack campaigns or bad actor groups

ARBOR® NETWORKS

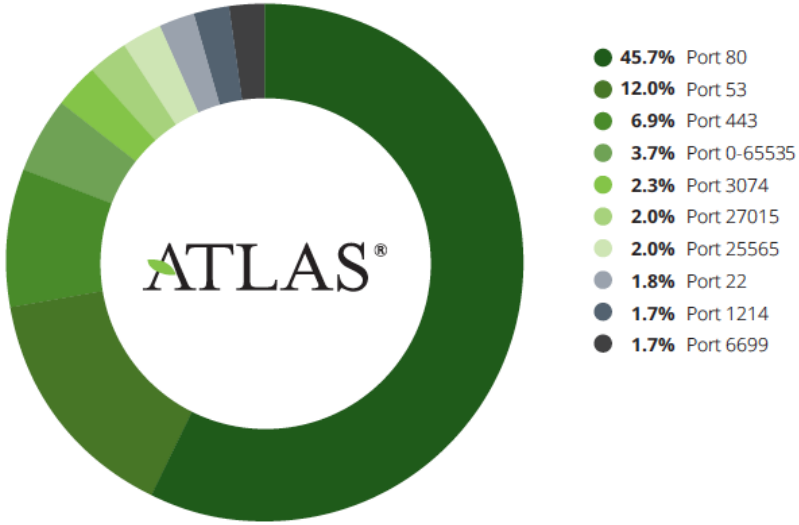
Attack duration & Target ports – ATLAS Perspective

- 91% of events lasted less than one hour
- Average attack duration was ~ 58 minutes
- Similar to last year

DDoS Attack Durations



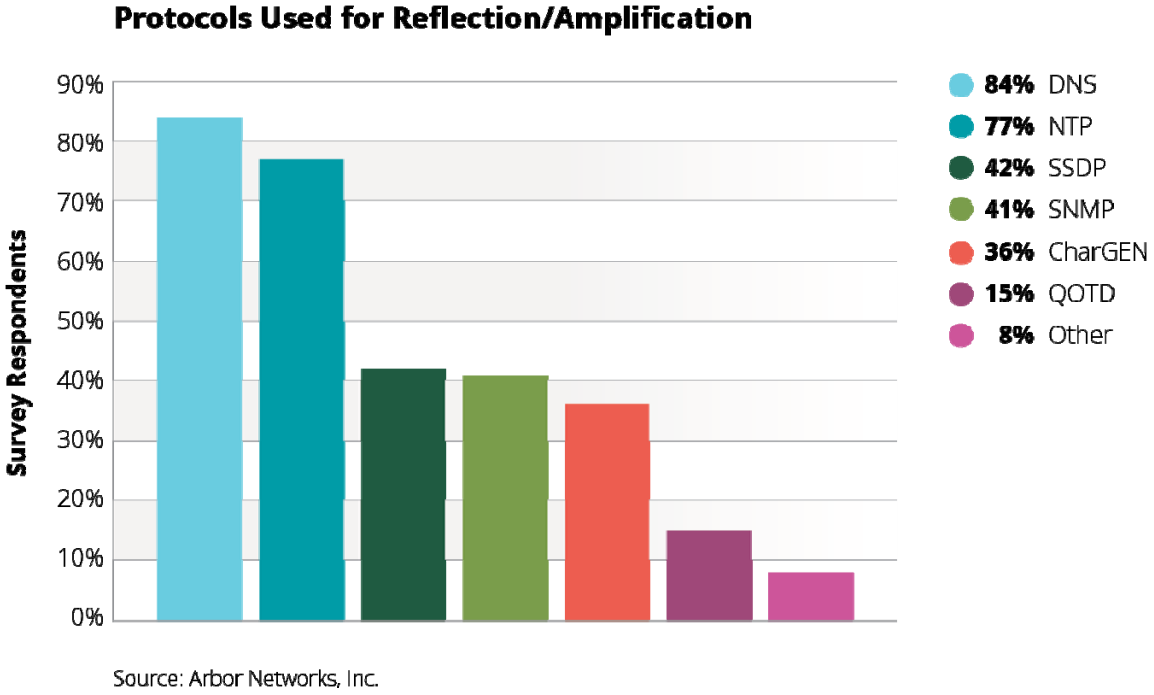
Ports Targeted by DDoS Attacks



- Top target service was again HTTP (port 80)
- Port 3074 (Xbox) & port 25565 (Minecraft) among the top 10 targets

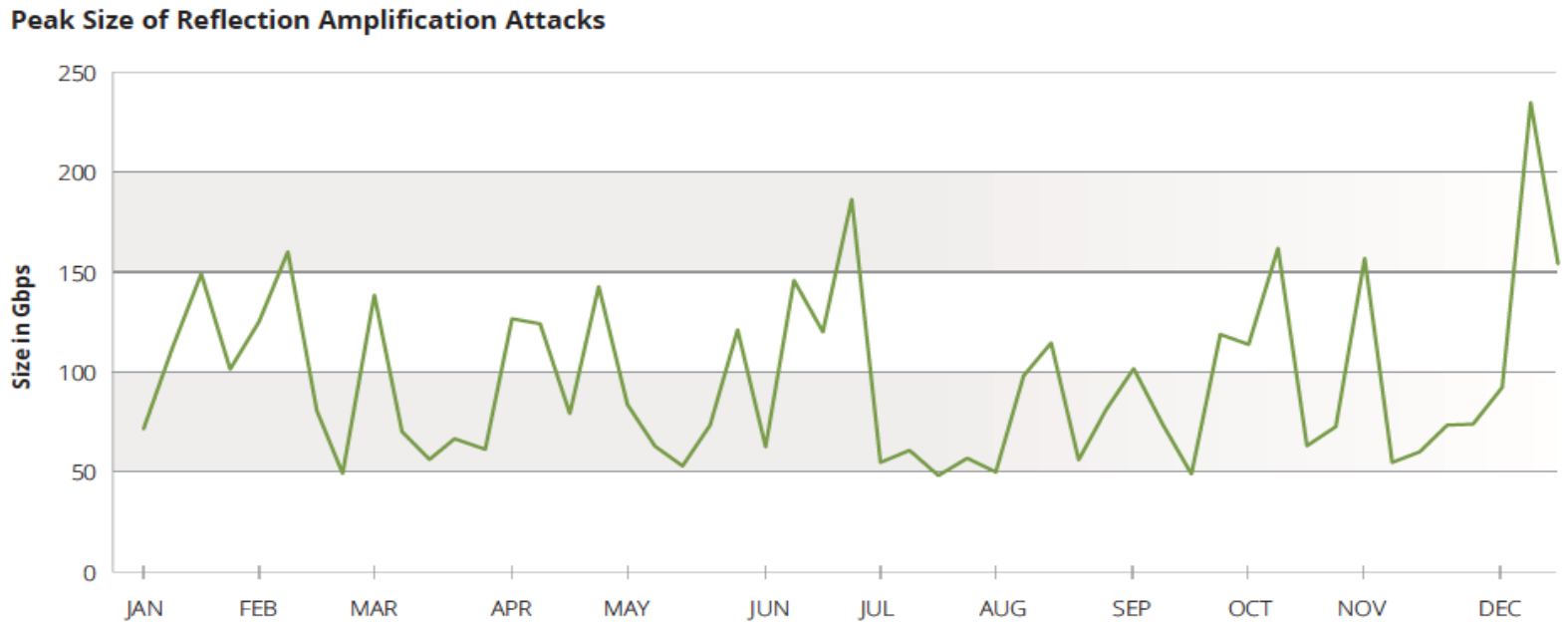
ARBOR® NETWORKS

DDoS – Reflection Amplification



- Reflection amplification attacks are still a key issue.
  - WISR respondents see DNS as most common protocol, closely followed by NTP.
  - Significant use of SSDP, SNMP and Chargen also reported.

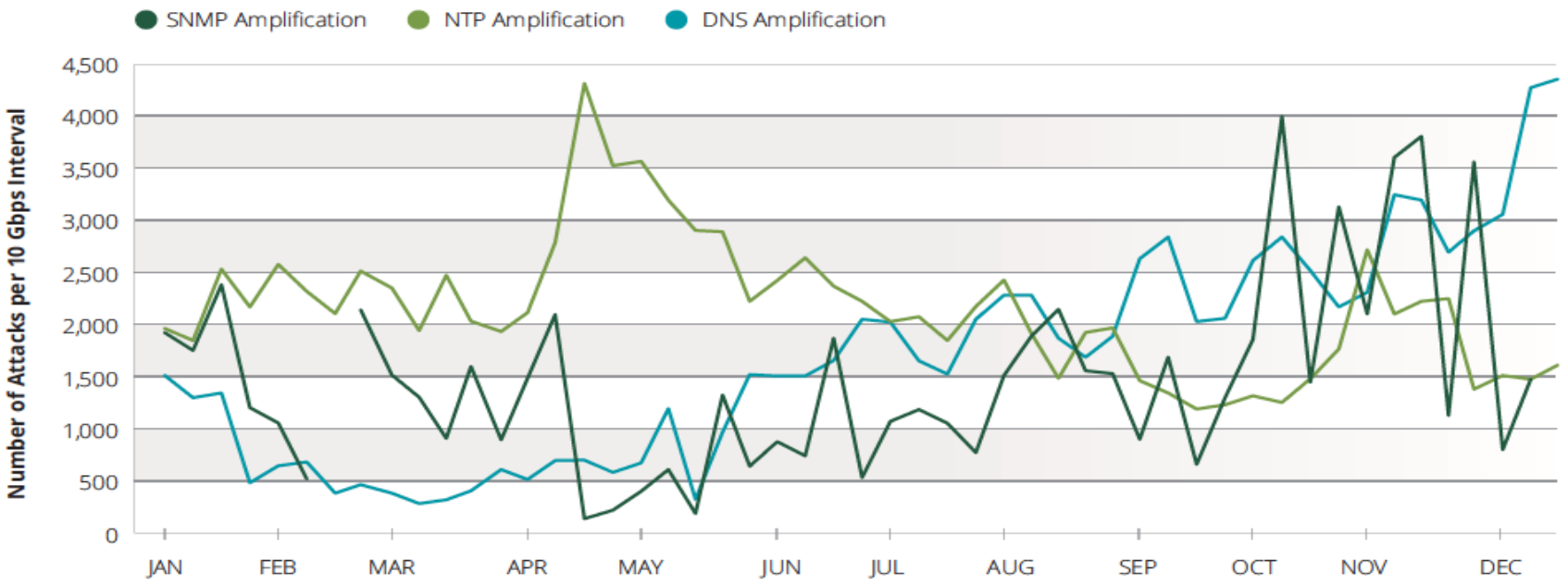
Reflection Amplification Attacks, ATLAS Perspective



- Reflection Amplification DDoS activities continuous increase in size and frequency
- Largest reflection amplification attack tracked in 2015 was an SSDP reflection attack at 252.64 Gbps
- Average size of reflection amplification attacks was around 1.97 Gbps, significantly above the more general average attack size.

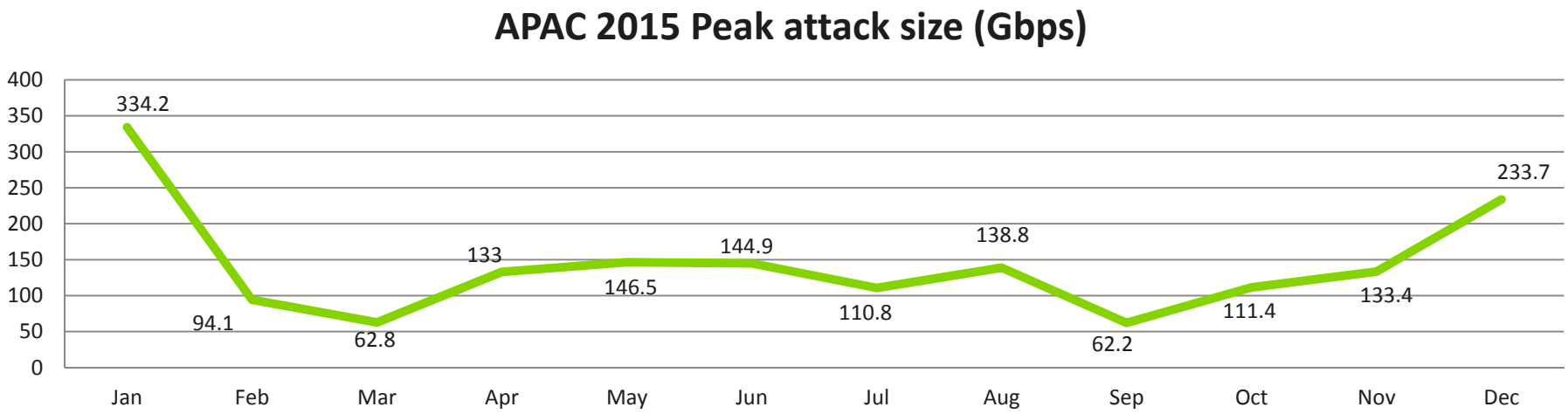
Reflection Amplification Attacks – ATLAS Perspective

Average Size Growth of DNS and SNMP Reflection Amplification Attacks



- NTP, SSDP and DNS are most commonly used protocols
- More than 50K SSDP attacks tracked per month in Q1
- More than 55K NTP attacks in Sept / Oct ’15
- Increase in the average size of attacks utilizing Chargen, SSDP and DNS

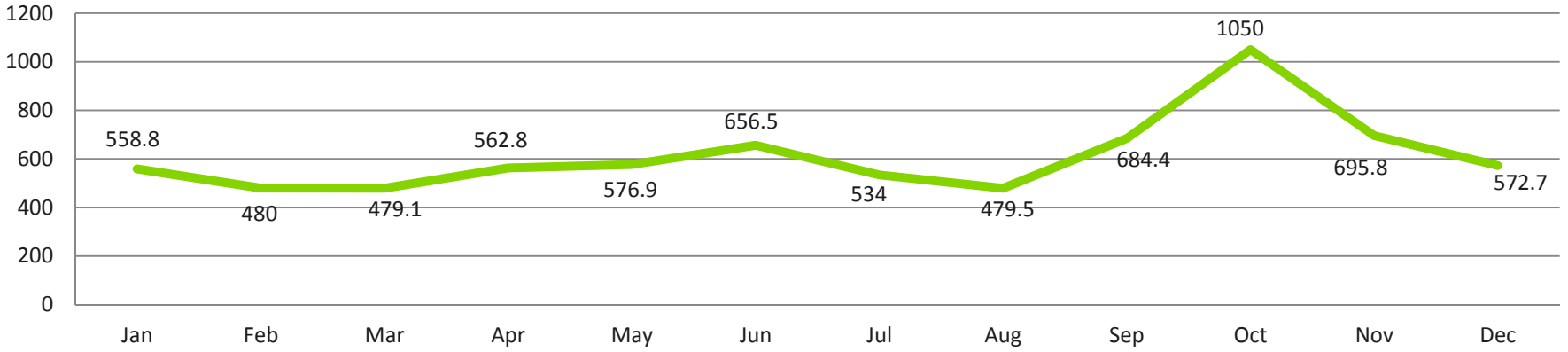
APAC DDoS attacks summary



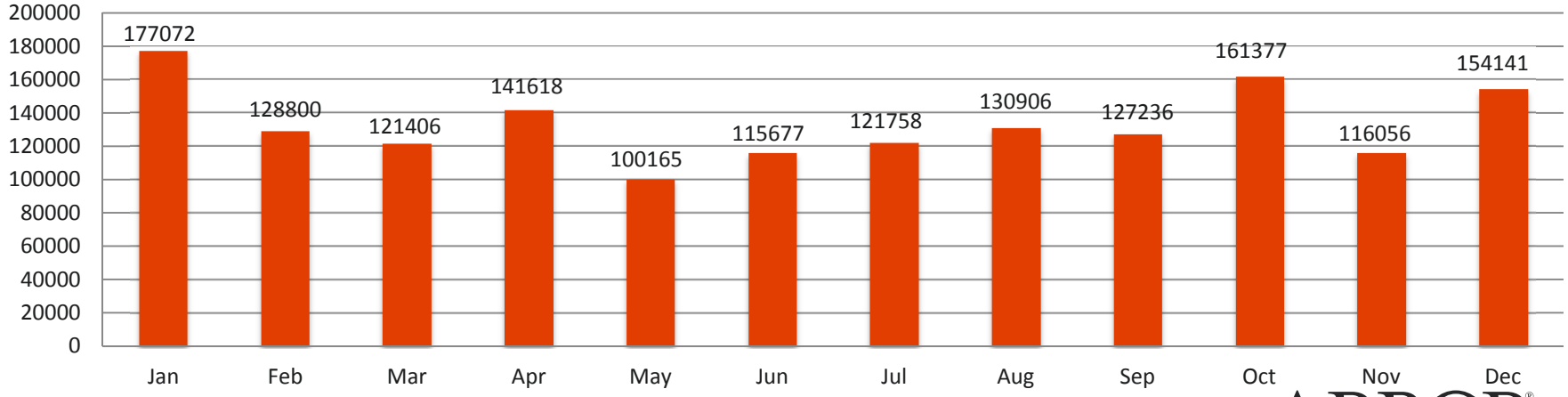
Q1 14	Q2 14	Q3 14	Q4 14	Q1 15	Q2 15	Q3 15	Q4 15
235Gbps/63 Mpps to India, NTP reflection attack, 21 min 23 sec	127Gbps/34 Mpps to Malaysia , NTP reflection attack, 29 min	99Gbps/26 Mpps to India, NTP reflection attack, 31 min	117Gbps/31 Mpps to India, NTP reflection attack, 15 min 37 sec	334.22Gbps /29.13Mpps to India, reflection attack, 6 min 45 sec	146.5Gbps/12.5Mpps to Korea, UDP flooding attack, 9 min 26 sec	139Gbps / 12.2Mpps to Laos, mixed reflection attacks, 1 hr 39 min	233Gbps / 66.4Mpps to Korea, NTP reflection attack, 28 min 39 sec

APAC DDoS attacks summary

APAC 2015 mean attack sizes (Mbps)

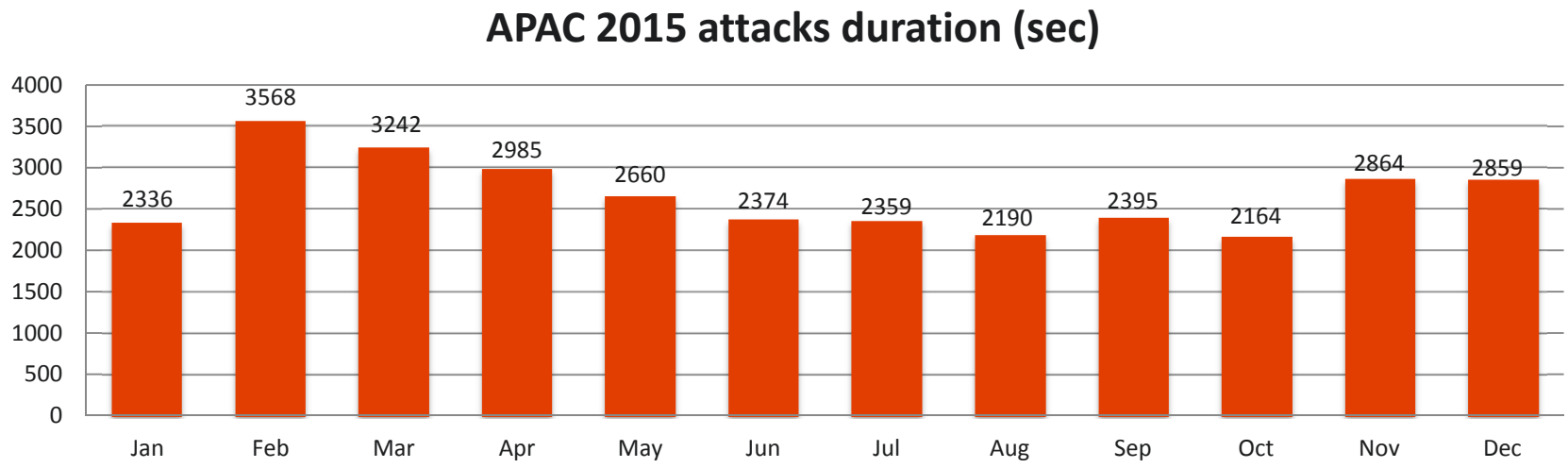


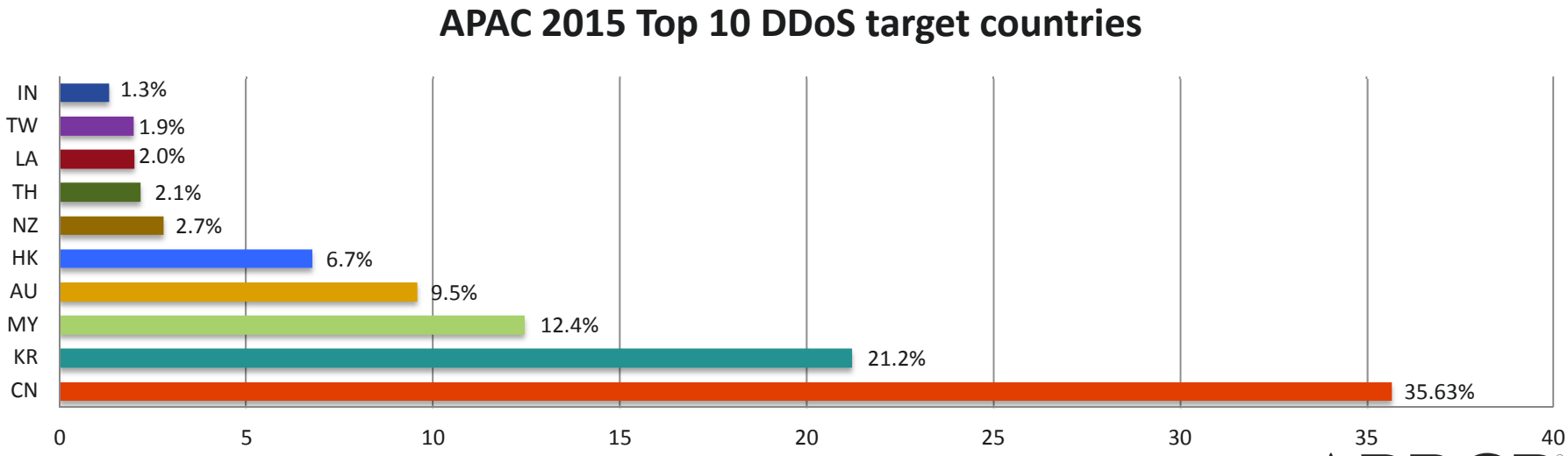
APAC 2015 no of DDoS attacks



ARBOR NETWORKS

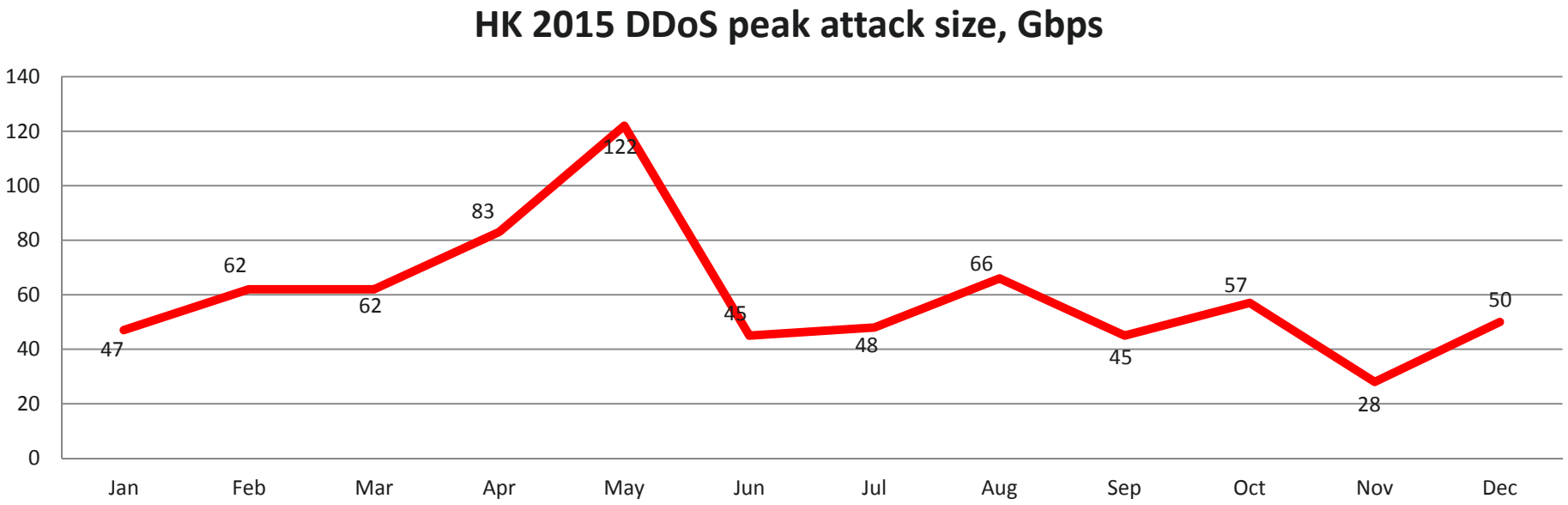
APAC DDoS attacks summary





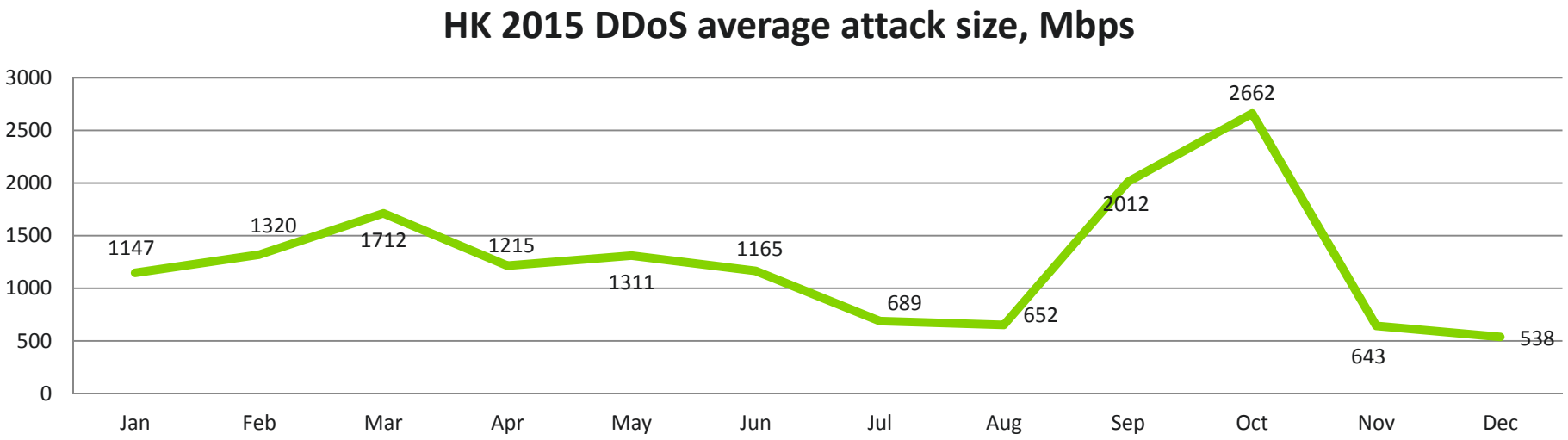
ARBOR NETWORKS

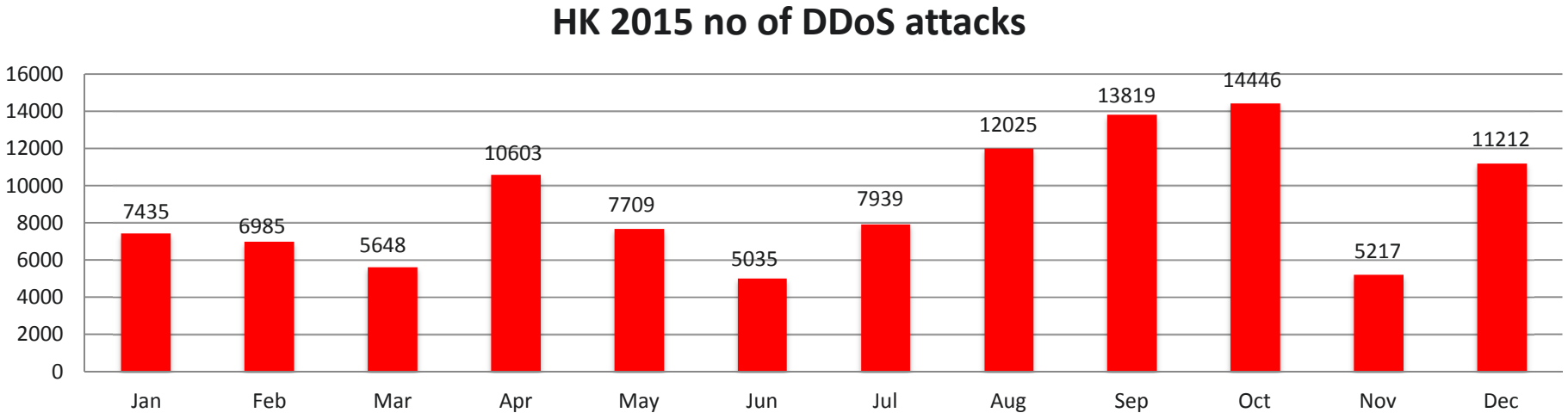
HK 2015 – DDoS attacks summary



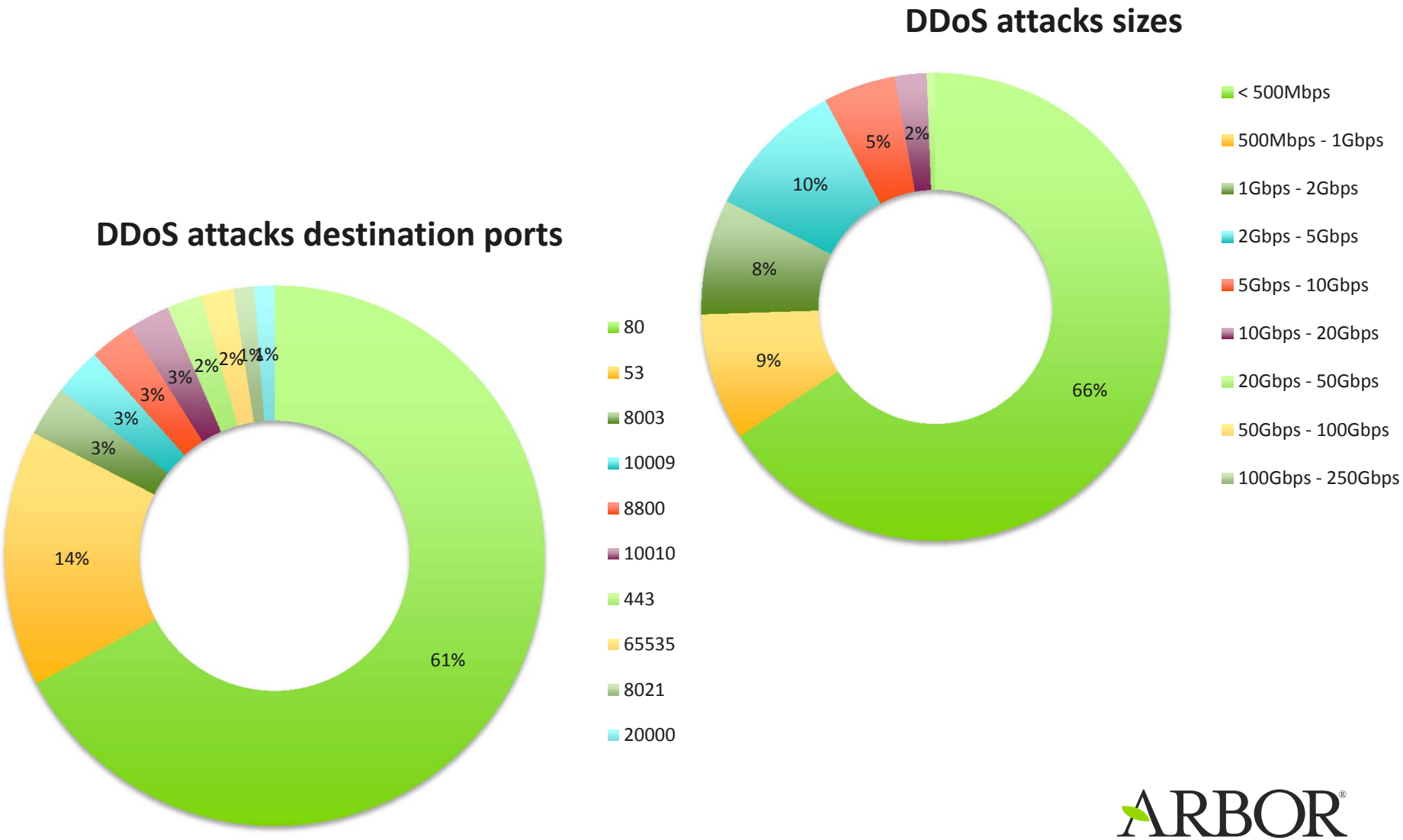
	HK	APAC
Peak attack size	122.46 Gbps	334.22 Gbps
Average attack size	1.34 Gbps	617.53 Mbps
Average duration	67 min 25 sec	44 min 11 sec
Attack dest port	Port 80	Port 80
Top reflection attack type	DNS	NTP

HK 2015 – DDoS attacks summary





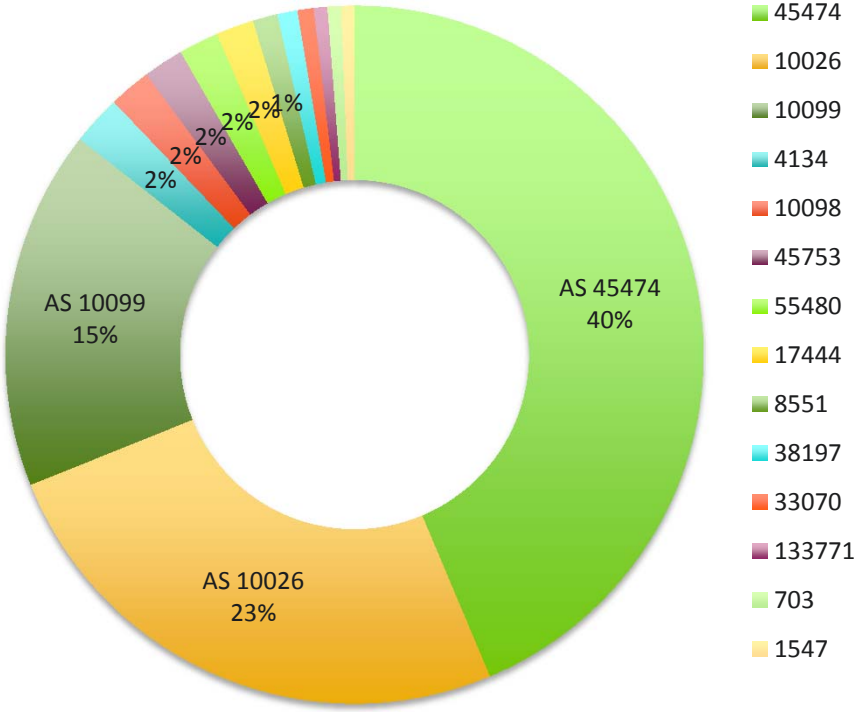
HK – DDoS attacks summary



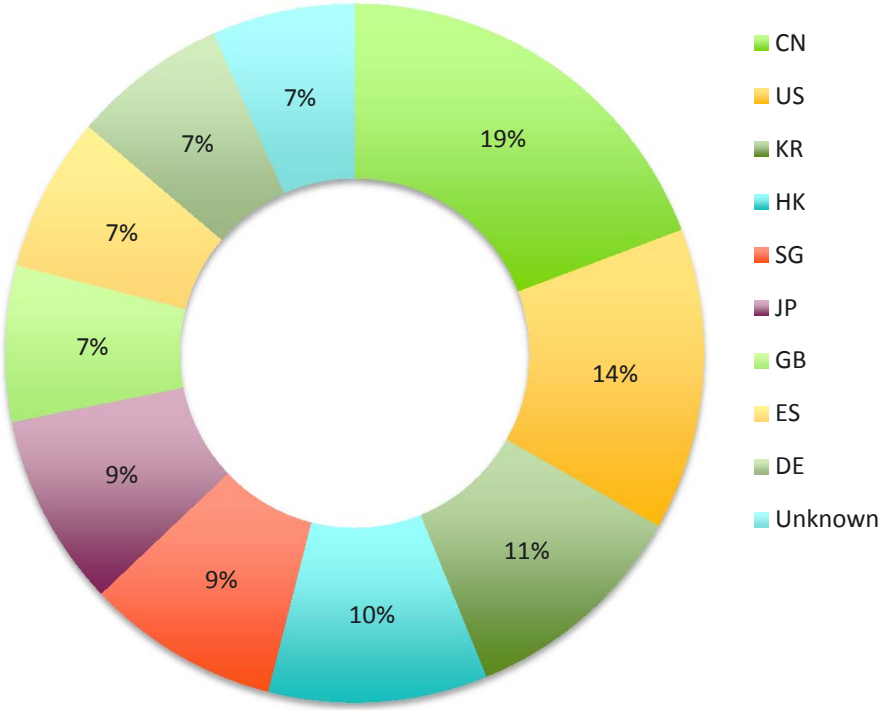
ARBOR NETWORKS

HK 2015 – DDoS attacks summary

HK 2015 DDoS attacks by ASN

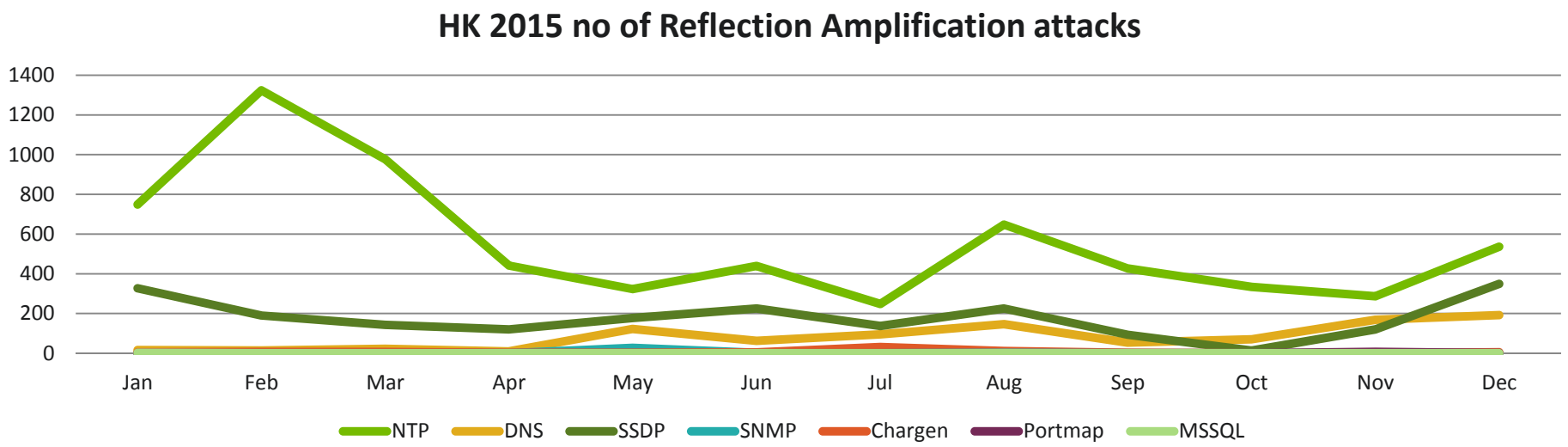


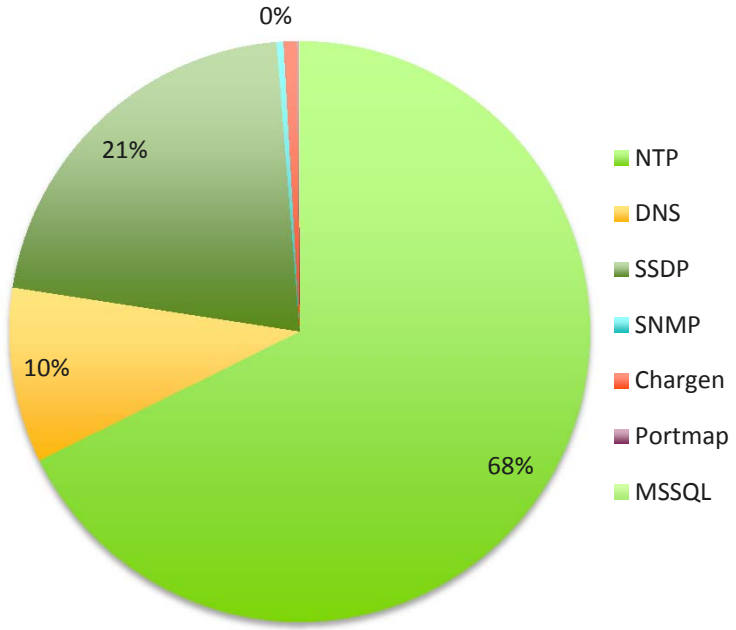
HK 2015 DDoS attacks source countries



ARBOR NETWORKS

HK 2015 - Reflection attacks





ARBOR NETWORKS

DD4BC – DDoS For Bitcoin

- A threat actor who launches DDoS extortion attacks against organizations, demanding payment to cease the attacks in Bitcoin.
- Currently the most notorious DDoS attacker in both the public and the operational security spheres.
- From July 2014, DD4BC extortion DDoS attacks have been observed.
- Throughout the year, increases in frequency and scope of DDoS extortion attempts
- DDoS extortions to low-level Bitcoin exchange, online casino, financial institutions
- Small (10-15Gbps) attacks as warning, reported to have seen attacks of size 40-60Gbps
- Claim to have 400-500 Gbps of DDoS capacity

DD4BC timeline

- First emerged in July 2014, debuted with DDoS extortion attempt against Bitcoin lotto sites
- Throughout the rest of 2014, DD4BC attacked various Bitcoin mining pools, Bitcoin exchanges, Bitcoin wallet providers, etc., mostly in Europe and North America.
- Most/all targets were Bitcoin-savvy.
- Extortion demands have ranged from 1 – 100 Bitcoins: approximately $227USD - $22,700USD.
- In 2015 Q2, DD4BC shifted its target base to financial institutions, as well as to e-commerce sites.
- So far, DD4BC has attacked financial institutions in Central and Western Europe, Switzerland, Guernsey, Iceland, North America (relatively few), Australia, New Zealand, and Japan.
- Most of the financial institutions attacked so far have been mid-tier and smaller, with only a few considered to be first-tier.

DD4BC extortion process

- Unannounced DDoS attack against targeted organization, 10-15gb/sec, anywhere from 15 minutes to an hour in length.
- DD4BC then send email extortion demand providing detailed knowledge of DDoS attack, demanding payment within 24 hours.
- If the victim doesn't pay, follow-up email increases the amount of Bitcoin payout, and threatens another DDoS attack – up to 60gb/sec observed. DD4BC claim 400gb/sec of DDoS attack generation capability, but this hasn't been borne out, so far.
- DD4BC DDoSes some (not all) targets who don't pay, sends repeated emails demanding increased extortion payout amounts.
- DD4BC will increase the demanded extortion payouts if the target takes inadequate defensive measures.

DD4BC extortion process

- DDoS attacks persist anywhere from a few hours to 12 hours to a series of attacks over multiple days.
- If the DDoS attack is successfully thwarted, DD4BC will eventually give up and go away.
- Sometimes, DD4BC will target the same organization again, a few days or weeks later.
- On a couple of occasions, DD4BC has re-targeted the same organization dozens of times.

DD4BC TTP (Tactics, Techniques, Procedures)

- DD4BC first attacked targets with a mixture of NTP, SSDP, and DNS reflection/amplification attacks, with SYN-flooding mixed in, from time to time.
- As time progressed, NTP and SSDP reflection/amplification became the primary vectors, with occasional SYN-floods.
- NTP and SSDP reflection/amplification vectors are sometimes used simultaneously.
- DD4BC concentrates attacks on the Web sites of targeted organizations.
- It appears that DD4BC has settled on utilizing commercial 'booter'/'stresser' services to launch DDoS attacks.
- As various booter/stresser services have expanded their attack offerings, DD4BC has broadened its DDoS attack methodologies to include chargen reflection/amplification and WordPress XMLRPC 'pingback' DDoS attacks.
- DD4BC will react to successful DDoS defense, varying attack methodologies (SSDP to NTP to SYN-flooding to WordPress XMLRPC 'pingback) and increasing attack bandwidth.

DD4BC extortion demand

From: "DD4BC Team" <dd4bc@Safe-mail.net>
Date: Mon, 16 Feb 2015 14:13:40 +0000
Subject: Re: DDOS ATTACK!

Return site back online without paying me first, it's going down again (protection will not help) and price to stop it increases to 3 BTC. And will keep doubling for every day of attack.

-------- Original Message --------

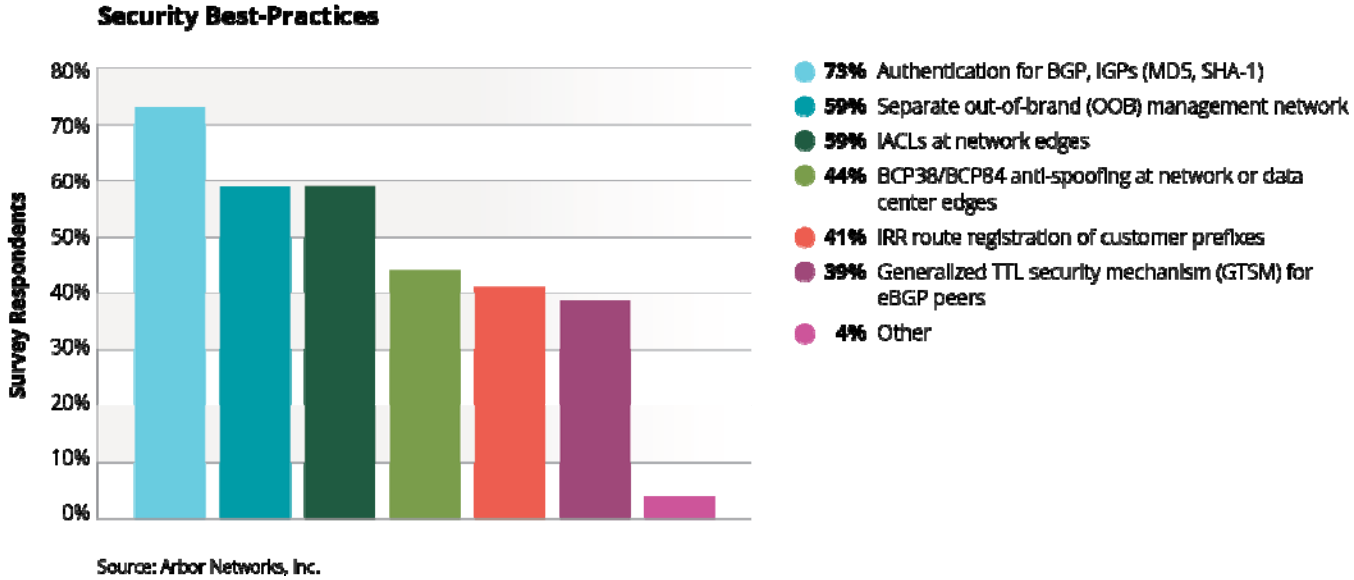
From: "DD4BC Team" <dd4bc@Safe-mail.net>
Subject: DDOS ATTACK!
Date: Sun, 15 Feb 2015 12:34:28 +0000

Hello,
Your site is extremely vulnerable to DDoS attacks.
I want to offer you info how to properly setup your protection, so that you can't be ddosed. If you want info on fixing it, pay me 1.5 BTC to 1E8R3cgnr2UcusyZ9k5KUvkj3fXYd9oWW6

Industry Best Current Practices (BCPs)

- BCPs are industry best practices for locking down a network
- Deploy these as policy to limit the exposure of your network
  - Separation of control plane from data plane
  - Interface ACLs (iACLs)
  - Source based remote triggered blackhole S/RTBH
  - Destination based remote triggered blackhole D/RTBH
  - Flowspec
  - Deploy **antispoofing** at *all* network edges.
    - **uRPF Loose-Mode** at the peering edge
    - **uRPF Strict Mode** at customer aggregation edge
    - **DHCP Snooping** and **IP Source Verify** at LAN access edge

Organizational Security Practices



- Implementation of anti-spoofing filters among service provider respondents is up to 44 percent this year, from 37 percent last year
  - Progress, but still less than half.
- Practice makes perfect
  - 31 percent of service providers (up from 21%) and 24% of EGE respondents now run DDoS incident rehearsals at least on a quarterly basis
- The proportion of service providers monitoring for route hijacks has also increased, up to 54 percent this year from 40 percent last year.