ARBOR NETWORKS

The Security Division of NETSCOUT

Arbor WISR XII
The Stakes Have Changed

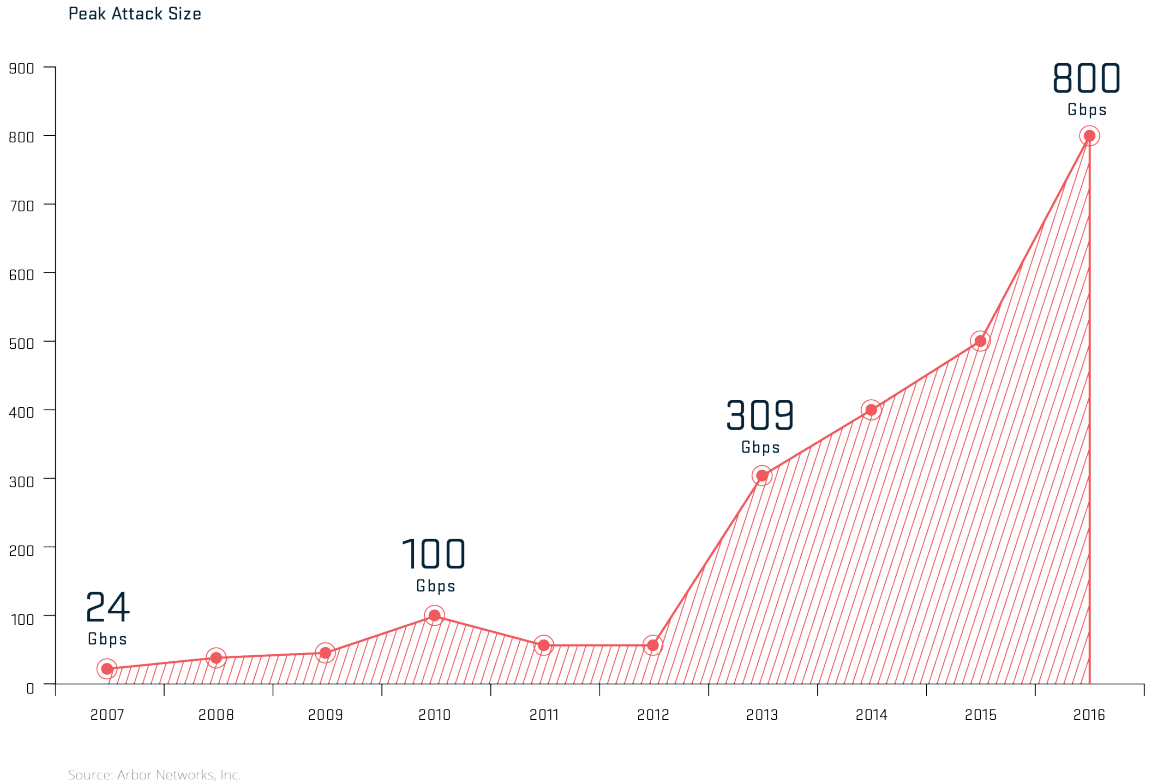
Julio Arruda

V1.0

Overview

This presentation provides a quick view of the ATLAS collected information for the year of 2016, then focus in Latin America targeted DDoS, and trends from 2015 to 2017

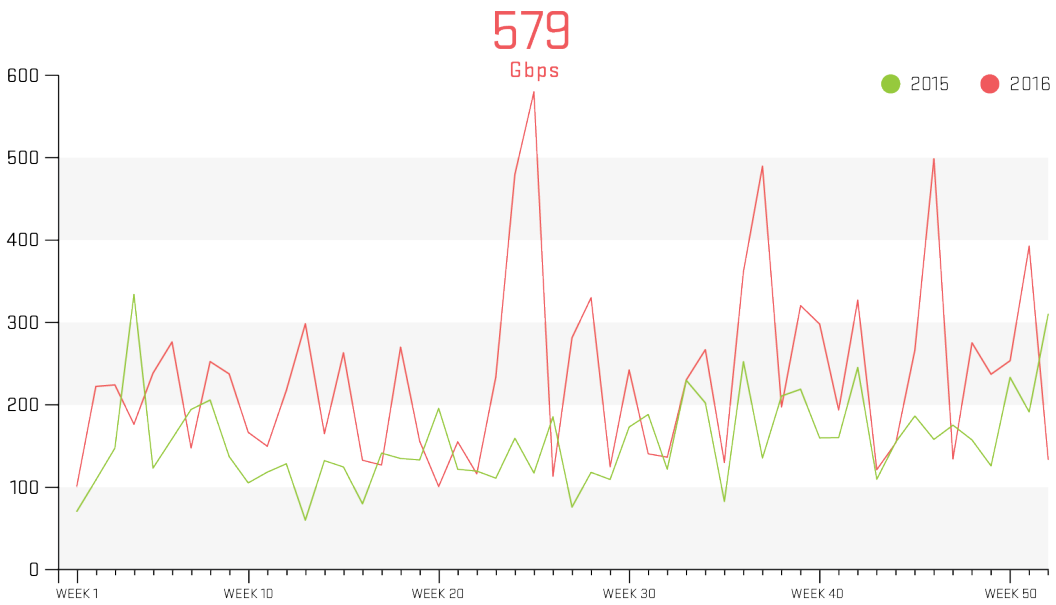
WISR Scale : Volumetric Attacks Increase



- 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
- Brazil had a record year again, with sustained +450Gbps attacks during the year, peaking at 540Gbps

Scale : The ATLAS Perspective

ATLAS Peak Monitored Attack Size (Gbps), 2015 vs. 2016



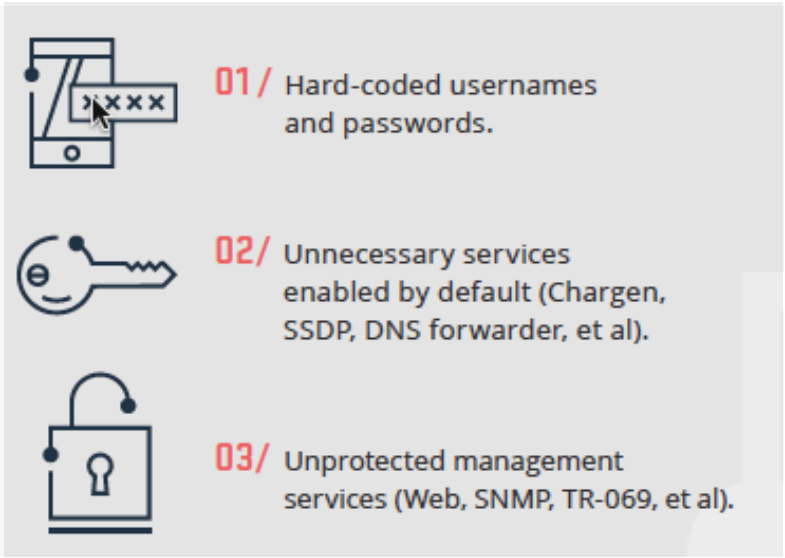
Source: Arbor Networks, Inc.

- Peak monitored attack of 579Gbps, 73% growth from 2015
- 558 attacks over 100Gbps, 87 over 200Gbps
  - Compared to 223 and 16 in 2015
- 20% of attacks over 1Gbps, as opposed to 16% in 2015
- Average attacks size now 931Mbps, up from 760Mbps, a 23% increase

Scale: Driving Factors, IoT

The Problem

- Almost every piece of technology we buy is ‘connected’
- Devices are designed to be easy to deploy and use, often resulting in limited security capabilities
- Software is very rarely upgraded. Some manufacturers don’t provide updates, or the ability to install updates

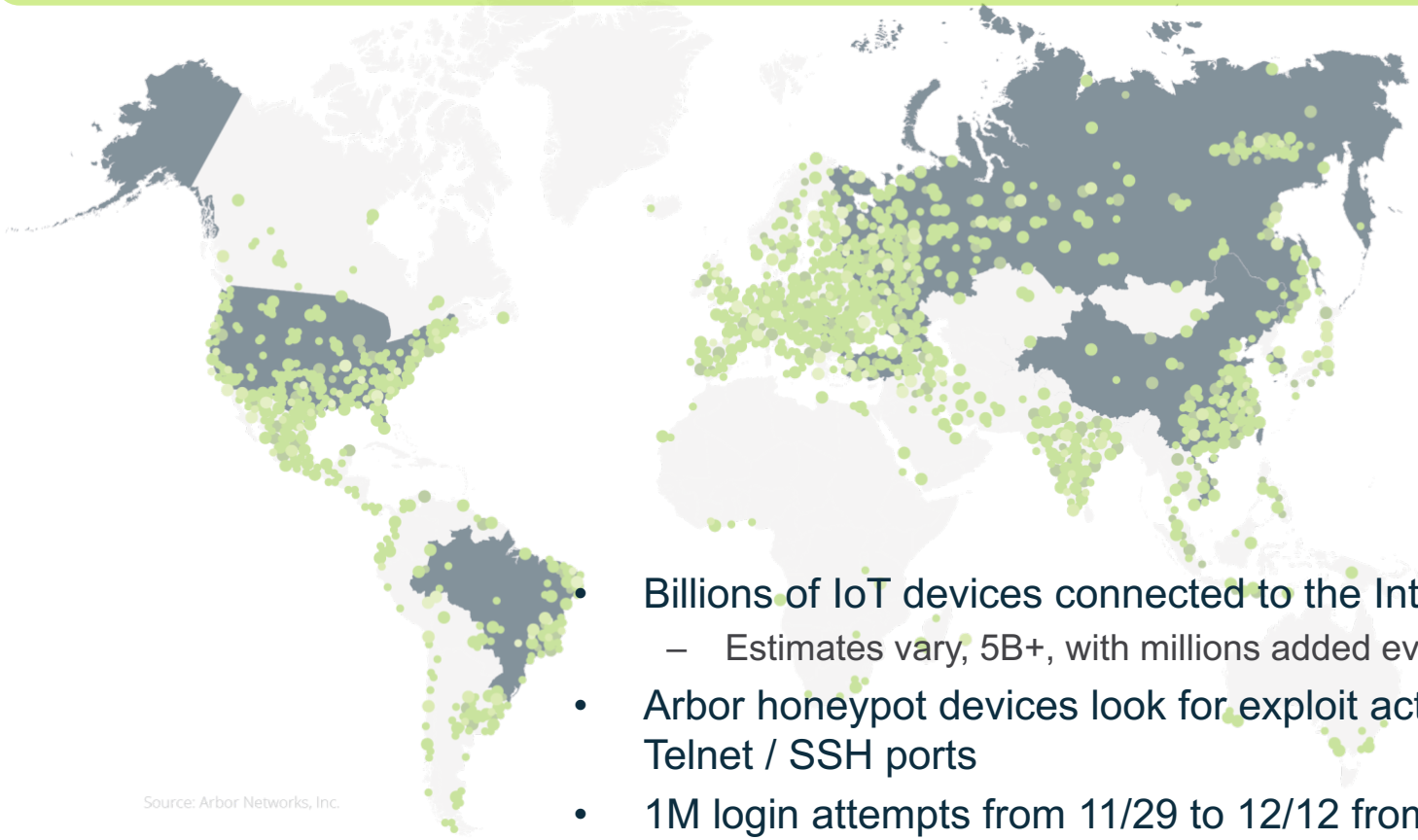


The Result

- First high-profile attack using IoT devices Christmas 2013, using CPE and webcams
- In 2016 Botnet owners started to recruit IoT devices en mass
- Attacks of 540Gbps against Brazil Large Sports Event, 620Gbps against Krebs, Dyn etc..

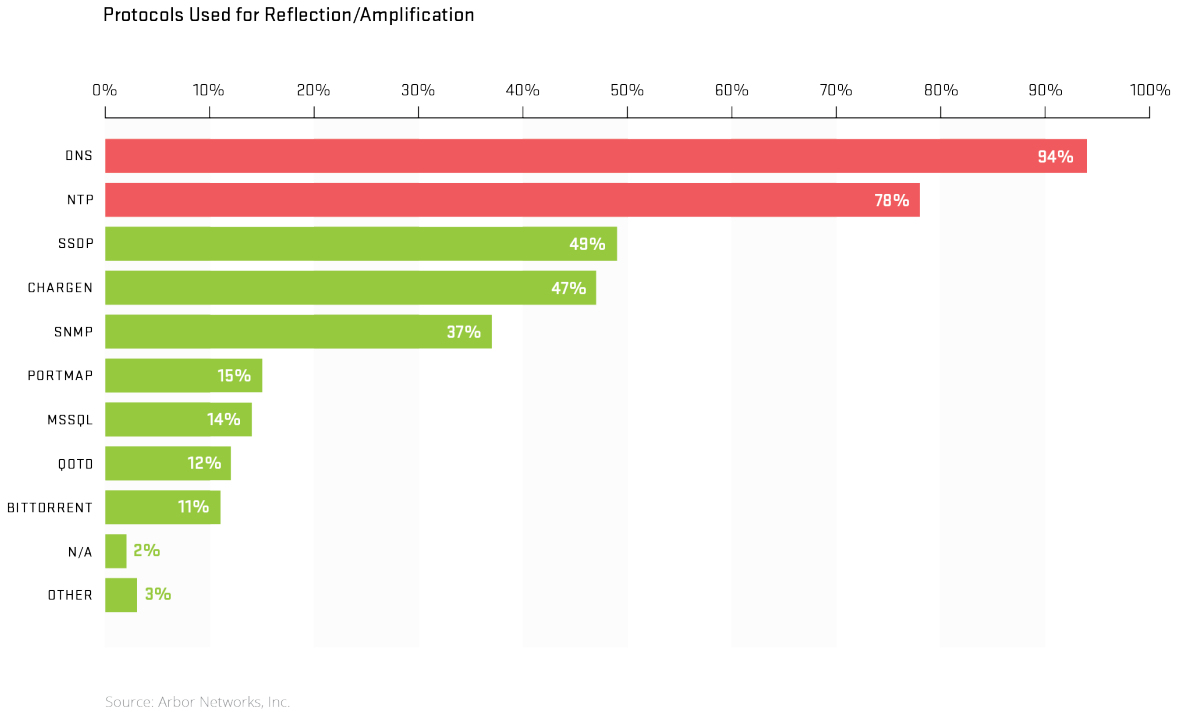
Scale: Driving Factors, Mirai

Mirai is designed to infect and control IoT devices and contains the code necessary to manage and build large-scale botnets



- Billions of IoT devices connected to the Internet
  - Estimates vary, 5B+, with millions added every day
- Arbor honeypot devices look for exploit activity on Telnet / SSH ports
- 1M login attempts from 11/29 to 12/12 from 92K unique IP addresses
- More than 1 attempt per minute in some regions

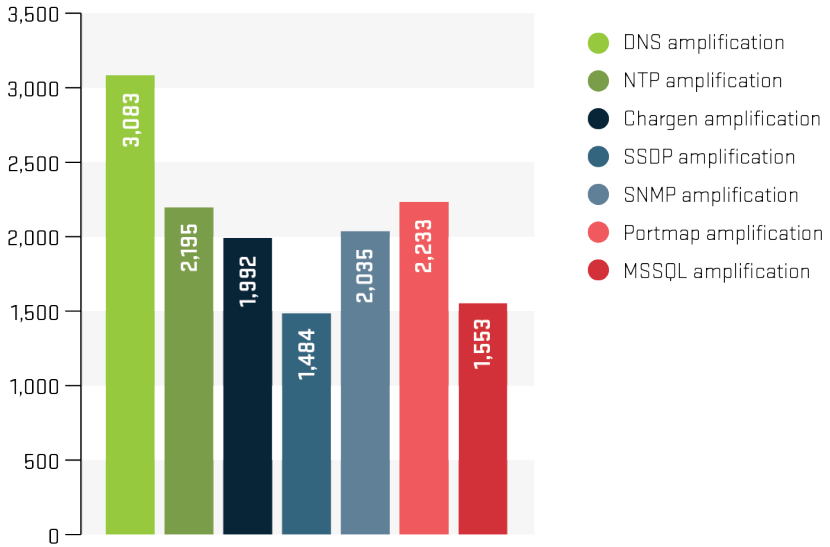
Scale: Driving Factors, Reflection Amplification



- 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

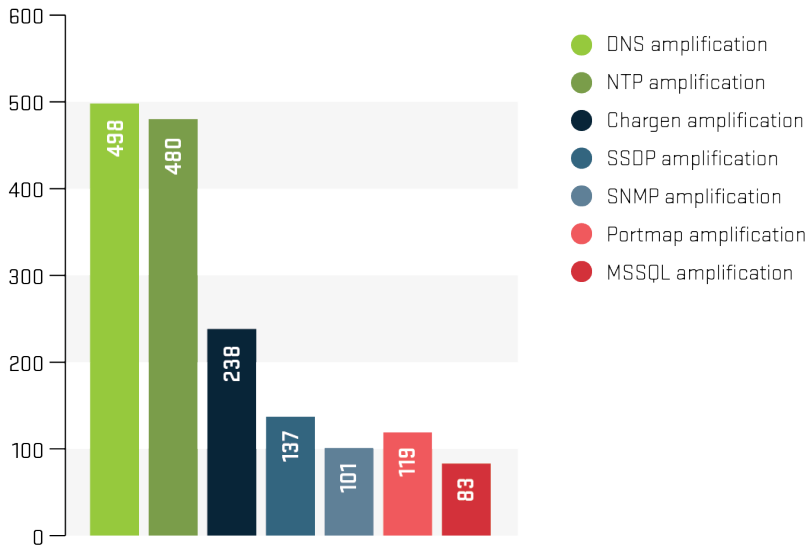
Scale: Driving Factors, Reflection Amplification

ATLAS Reflection/Amplification Attacks, Average Attack Size (Mbps)



Source: Arbor Networks, Inc.

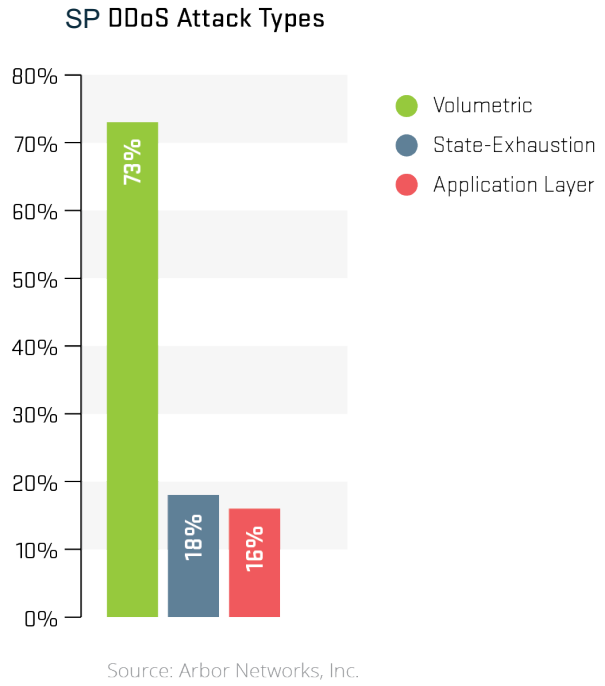
ATLAS Reflection/Amplification Attacks, Peak Sizes (Gbps)

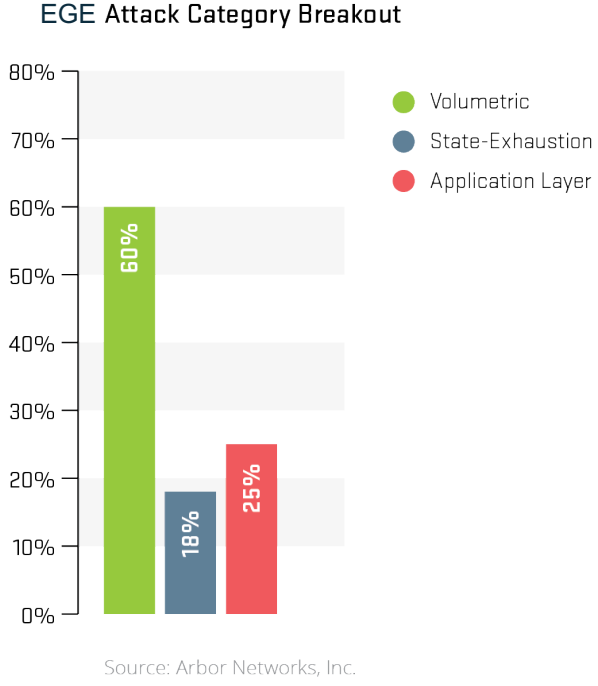


Source: Arbor Networks, Inc.

- 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

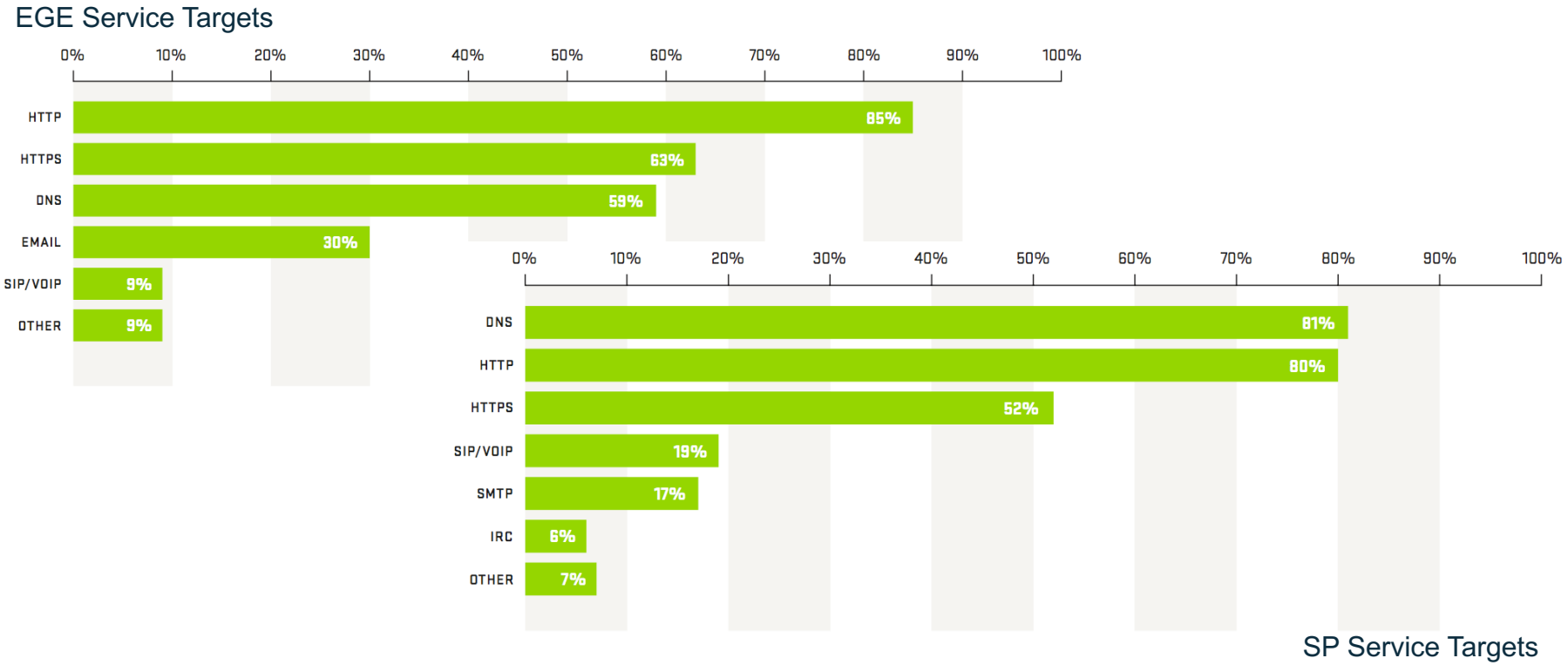
Complexity : Attack Types





- Volumetric attacks still represent the majority of activity for both SP and EGE respondents
- 95% of SP report applications layer attacks, 93% last year, 90% in 2014
- 67% of SP report multi-vector attacks, 56% last year, 32% in 2014

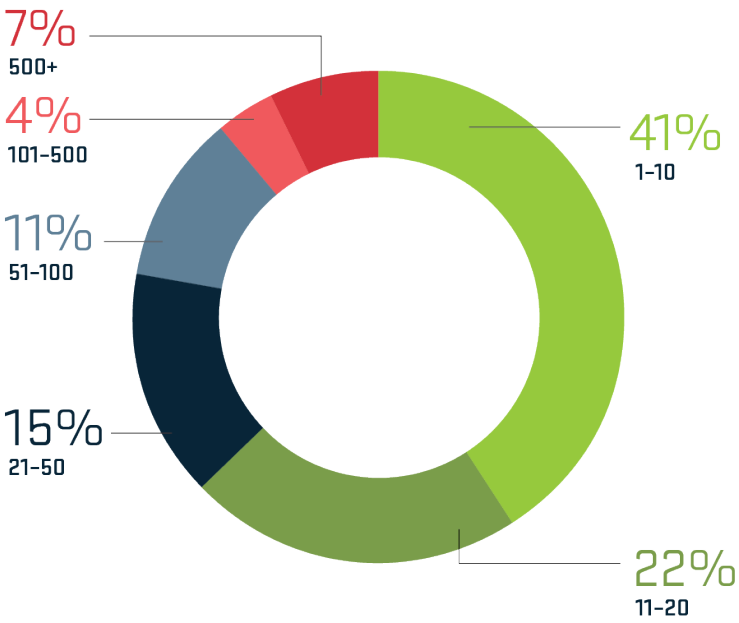
Complexity : Targeted Services



- DNS and HTTP the most common services targeted by application later attacks
- Majority of SP and EGE respondents also see attacks targeting HTTPS
- 57% of EGE respondents see attacks targeting the application behind HTTPS
  - Much higher than the 22% seen by SPs
  - Cipher suites that prevent traffic inspection are a key problem

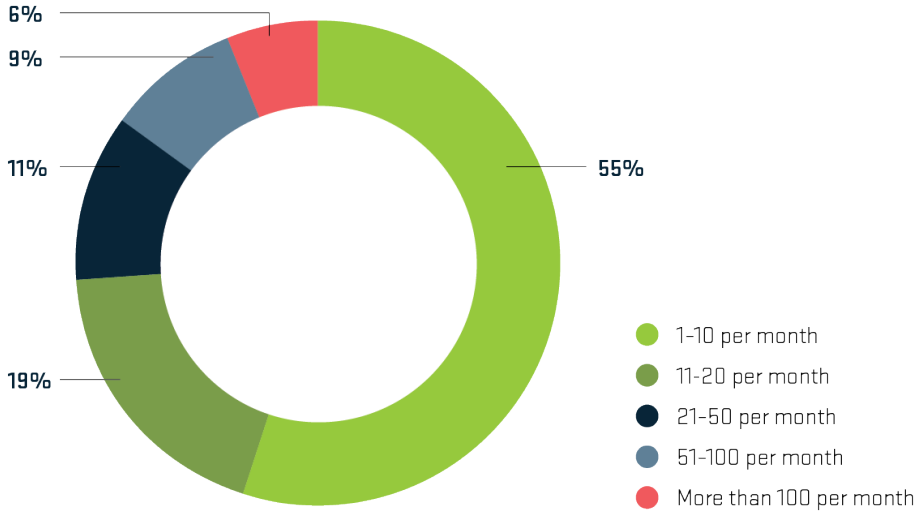
Frequency : Up Across the Board

Data Center Attack Frequency



Source: Arbor Networks, Inc.

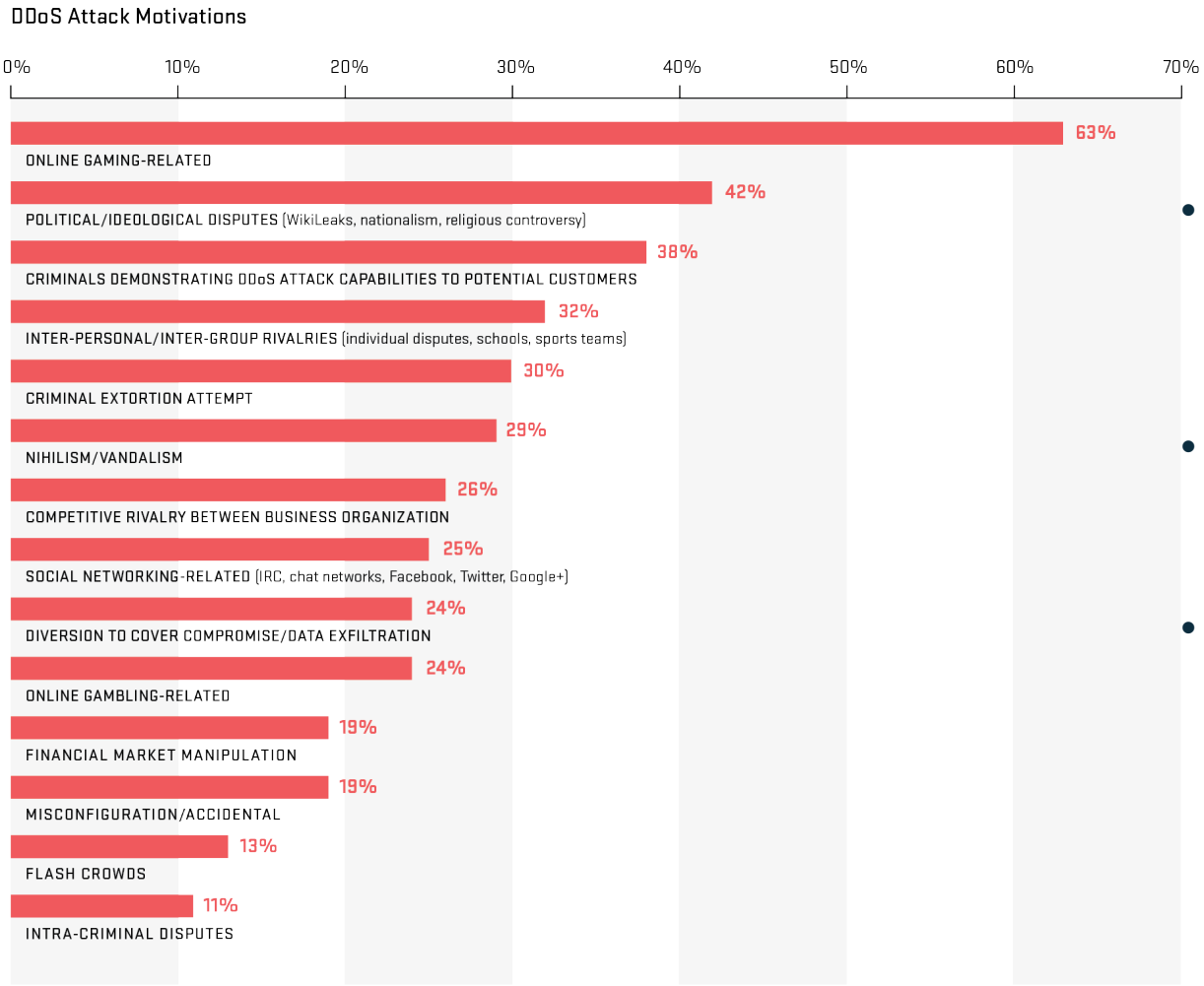
EGE Attack Frequency



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.

Motivations: Many and Varied

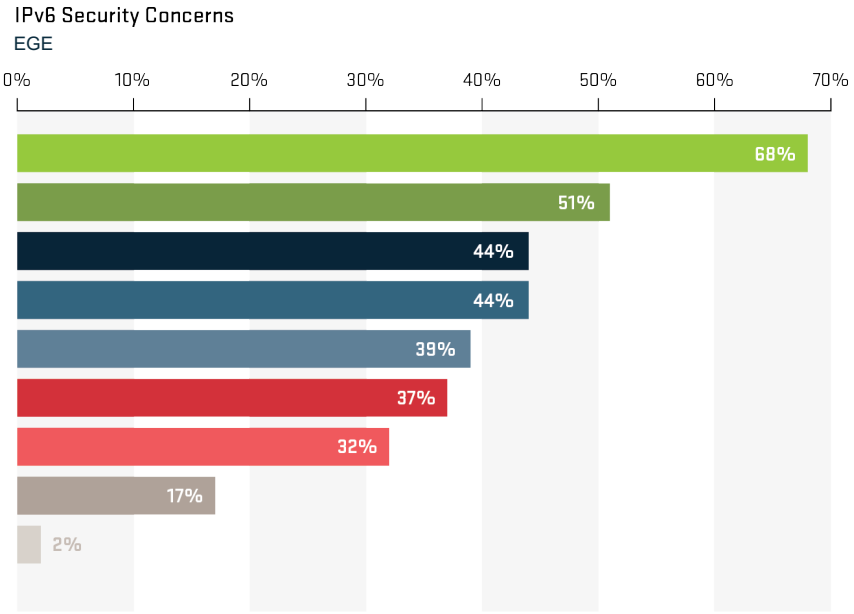


- SPs see Online Gaming and Hackivism as top motivations
- EGE see Ideological Hacktivism and Extortion as top
- 26% of EGE see DDoS for distraction, up from 12%

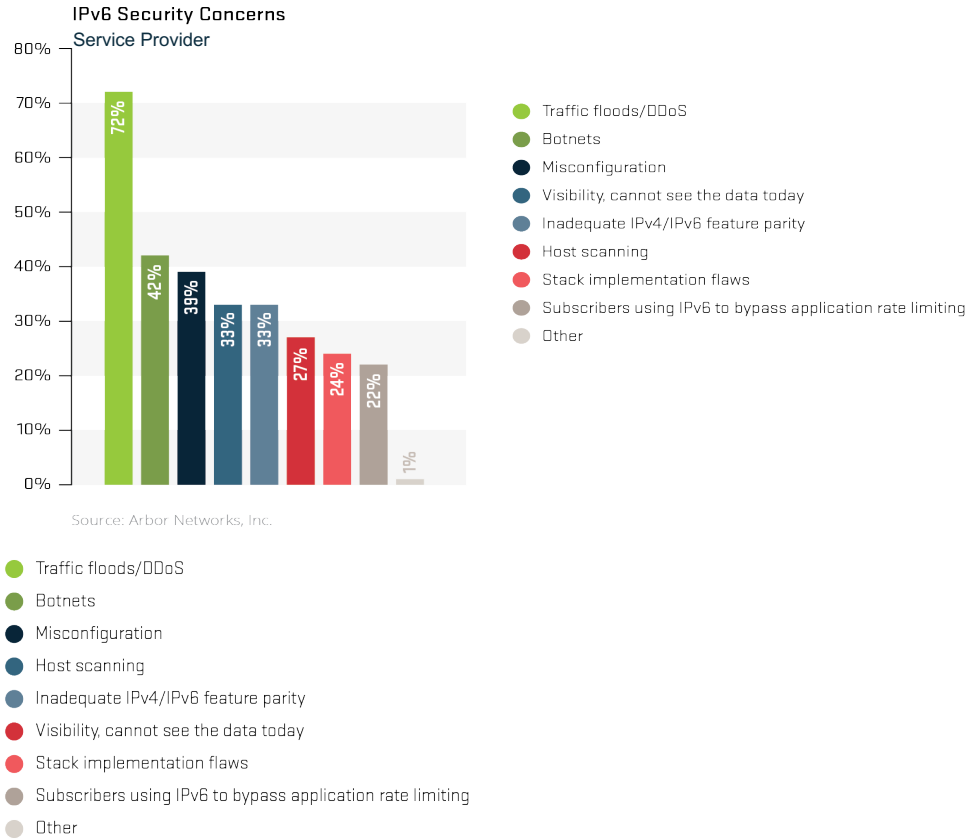
Source: Arbor Networks, Inc.

IPv6

- SP visibility is down 10%
  - IPv6 flow telemetry capability up to 53% from 43% last year
- Peak IPv6 traffic 6Tbps, up 20%
  - Predicted growth rates are low



Source: Arbor Networks, Inc.



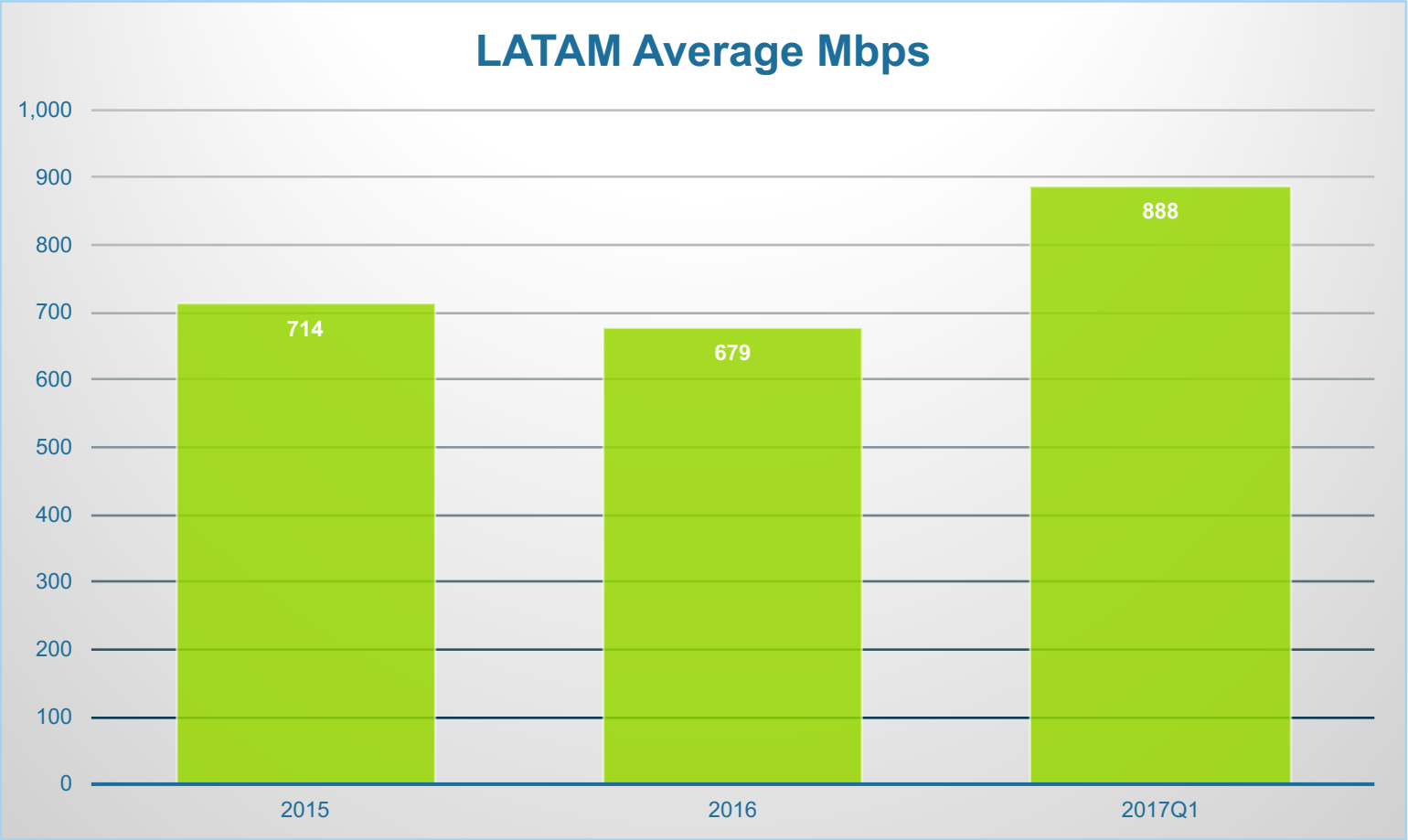
Source: Arbor Networks, Inc.

- Higher proportions of EGE offer services over IPv6 and use it on internal networks, 67% vs 58% and 67% vs 50%
- DDoS attacks are the top security concern for both SP and EGE

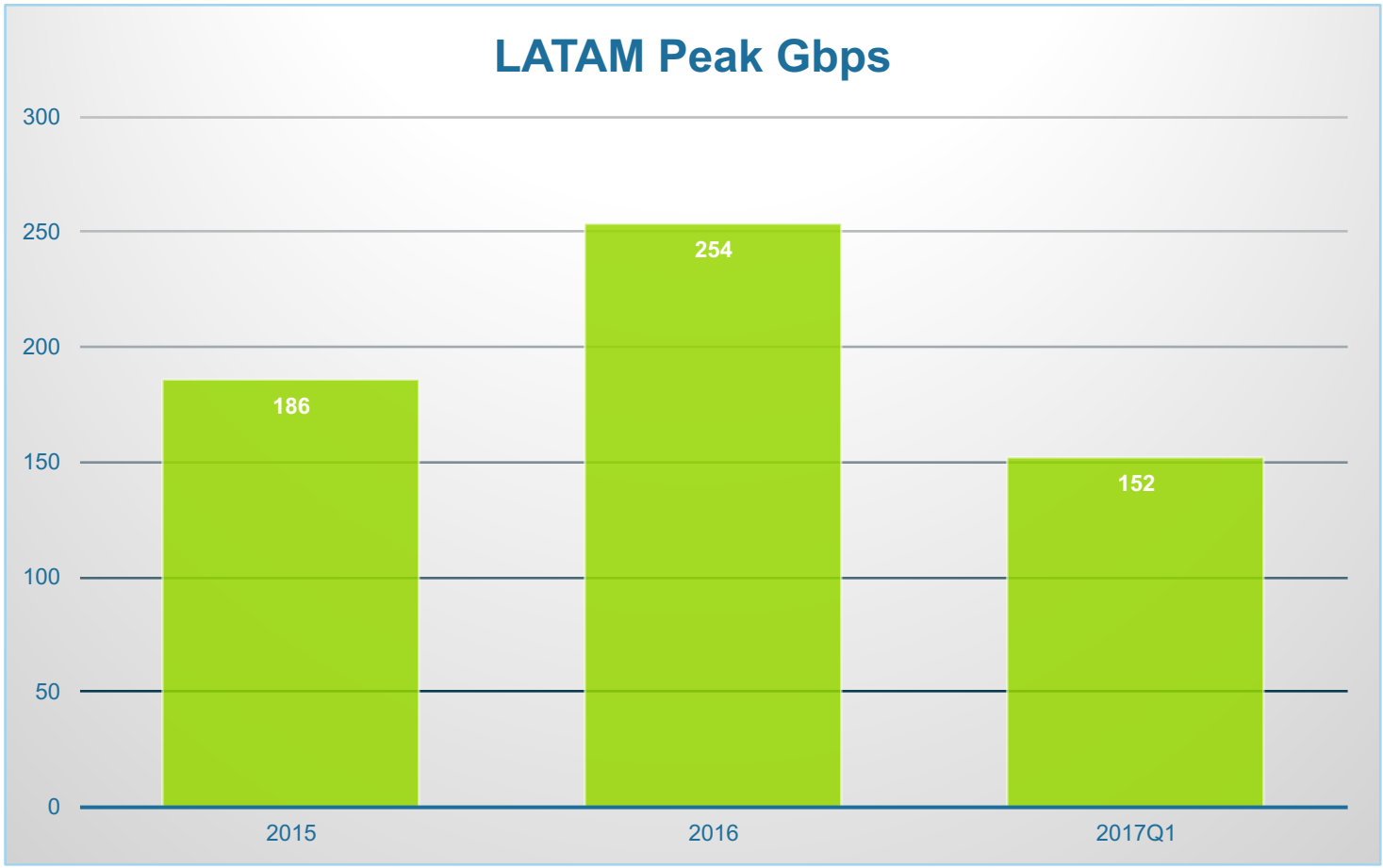
Countries with largest attacks ATLAS 2016

- Brazil – 254Gbps (Confirmed > 450Gbps in Large Sports Event, not in ATLAS)
- Argentina – 108Gbps
- Chile – 103Gbps
- Ecuador – 74Gbps
- Colombia – 72Gbps
- Mexico – 83Gbps

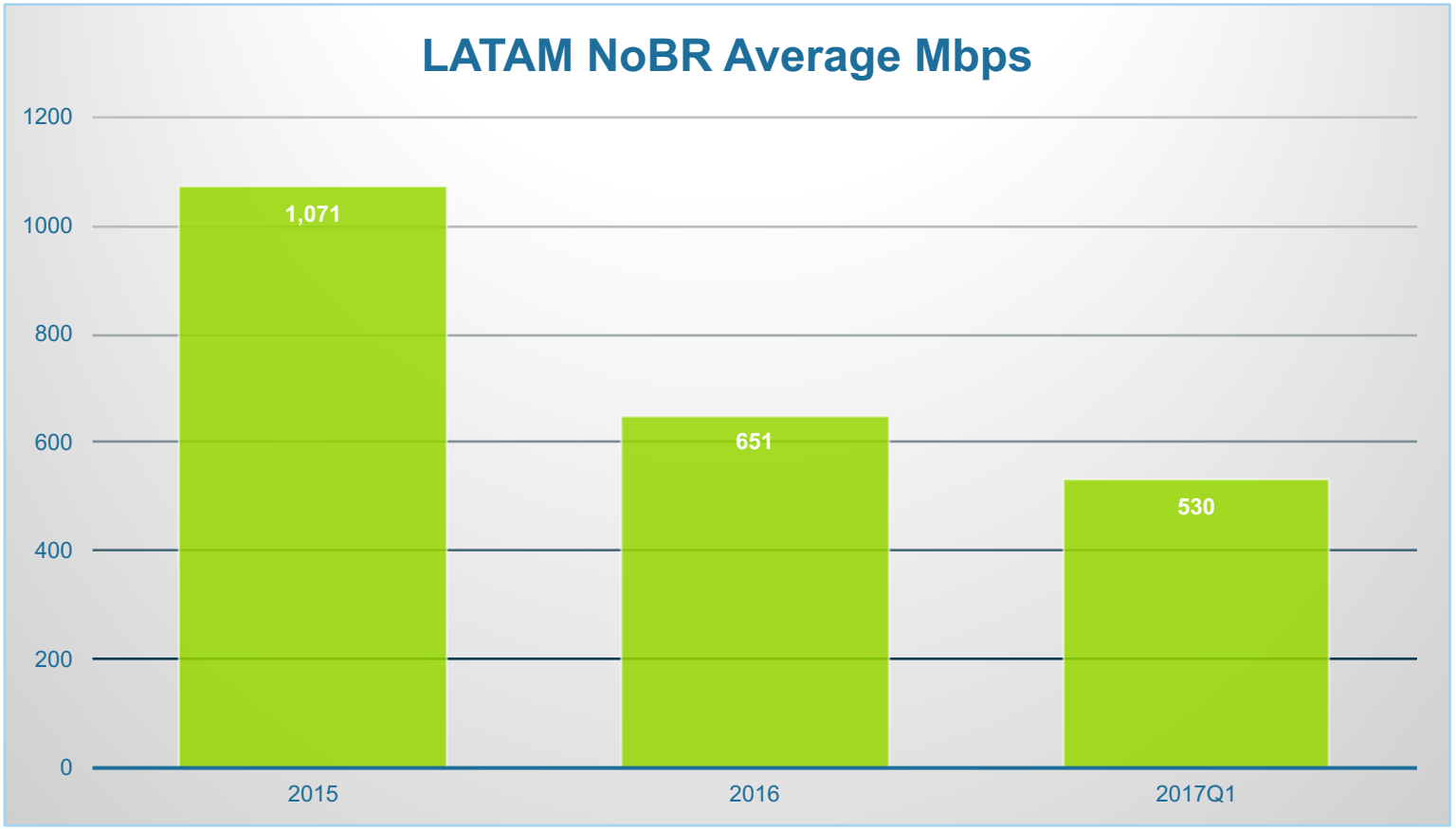
Averages including Brazil



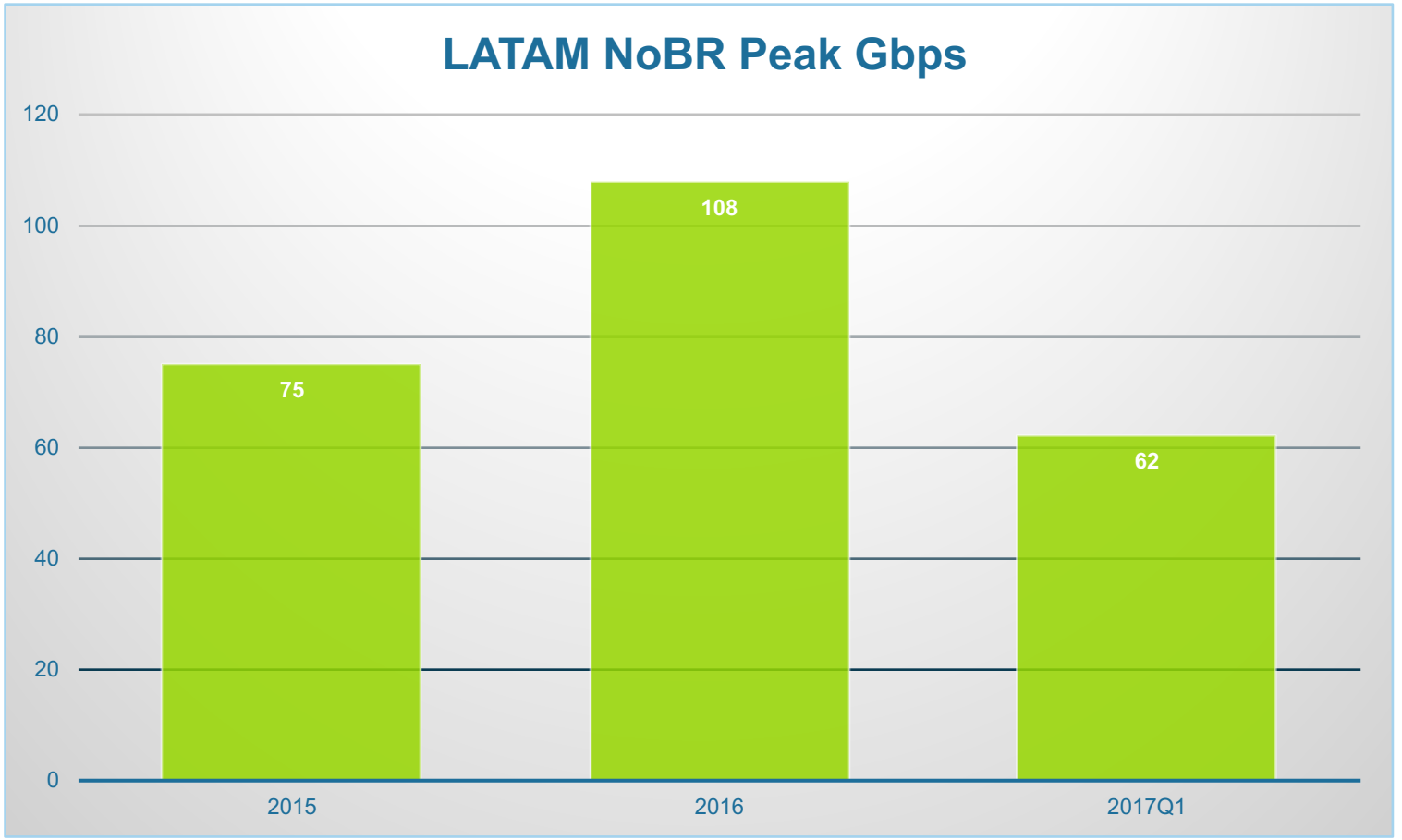
Peaks including Brazil



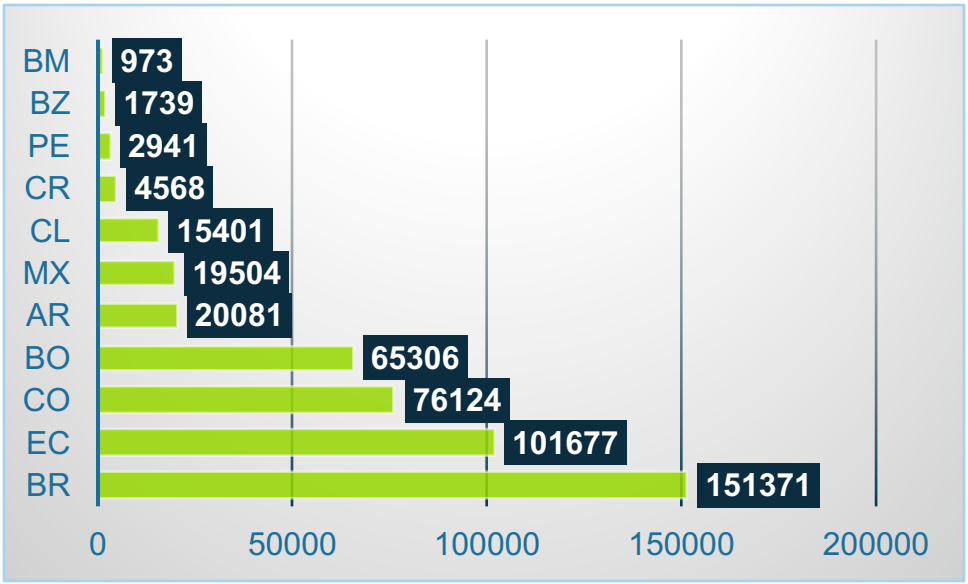
Averages Excluding Brazil

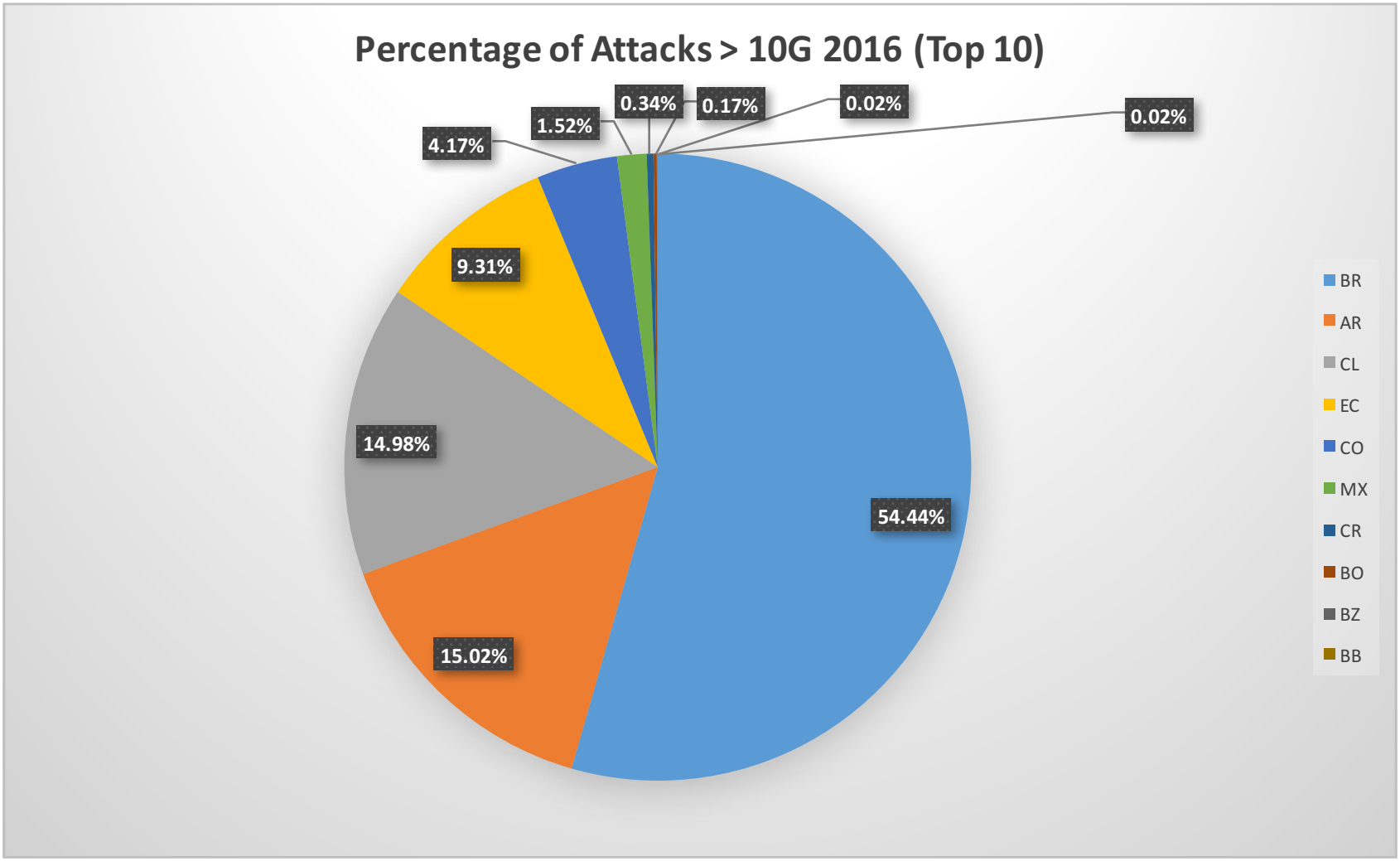


Peaks Excluding Brazil

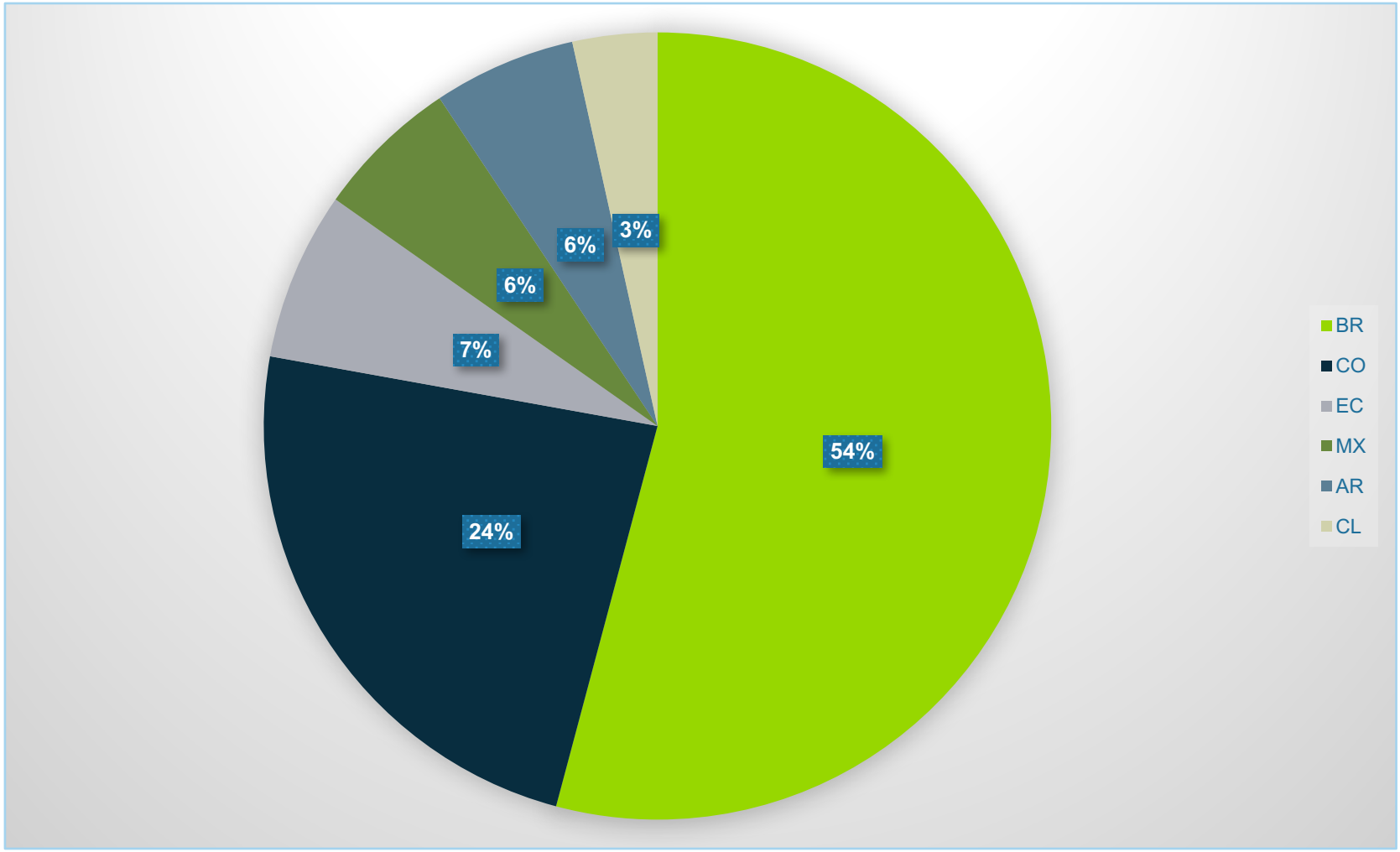


2016 Total Number of Attacks Per Top 11 Countries

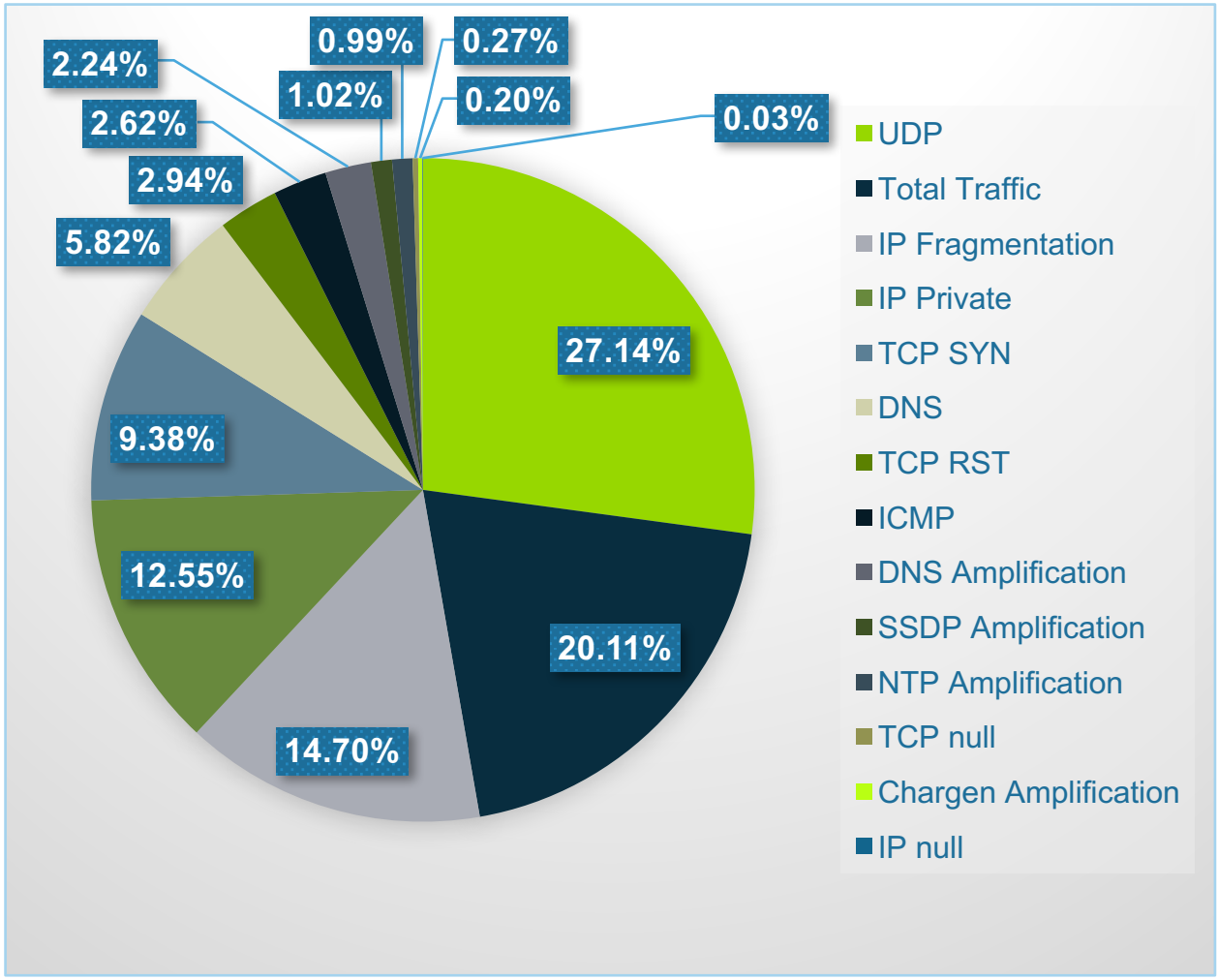




2016 Number of Attacks (Top 6)



Attack Types Breakout 2016



Questions?

Contact: jarruda@arbor.net

ARBOR NETWORKS
The Security Division of NETSCOUT