

NETSCOUT®

Guardians of the Connected World

Arbor

Worldwide Infrastructure Security Report Highlights

Gary Sockrider, Principal Security Technologist

Volume XIII

Kleber Carriello – Senior Consulting Engineer

Overview

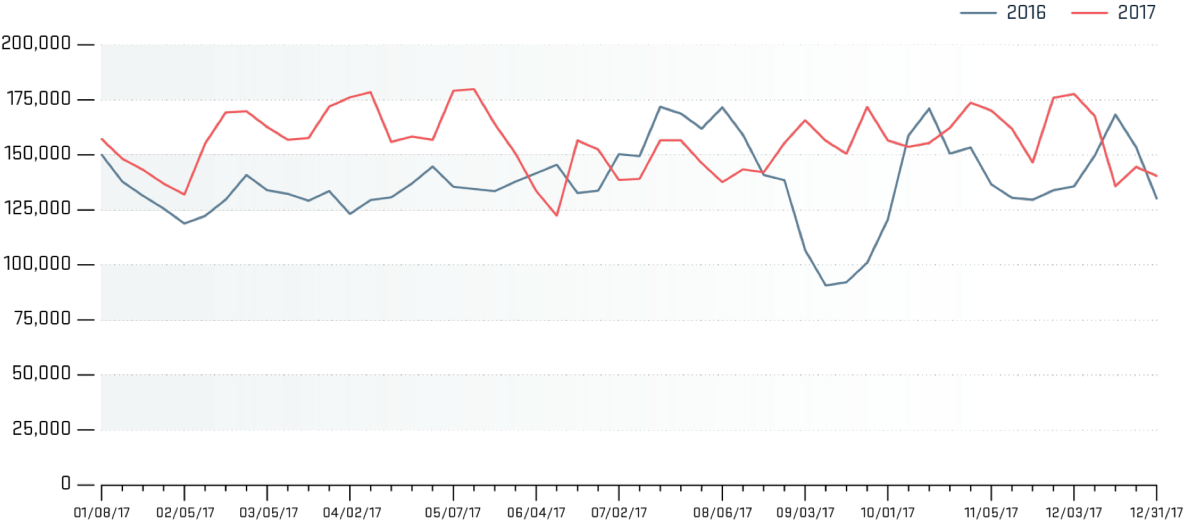
- This presentation provides a summary of NETSCOUT | Arbor's 13th annual Worldwide Infrastructure Security Report (WISR)
- The WISR features observations from network and security professionals at the world's leading service provider, cloud / hosting and enterprise organizations
- The report covers a comprehensive range of issues from threat detection and incident response to managed services, staffing, and budgets
- Its focus is on the operational challenges faced daily and the strategies adopted to address and mitigate them



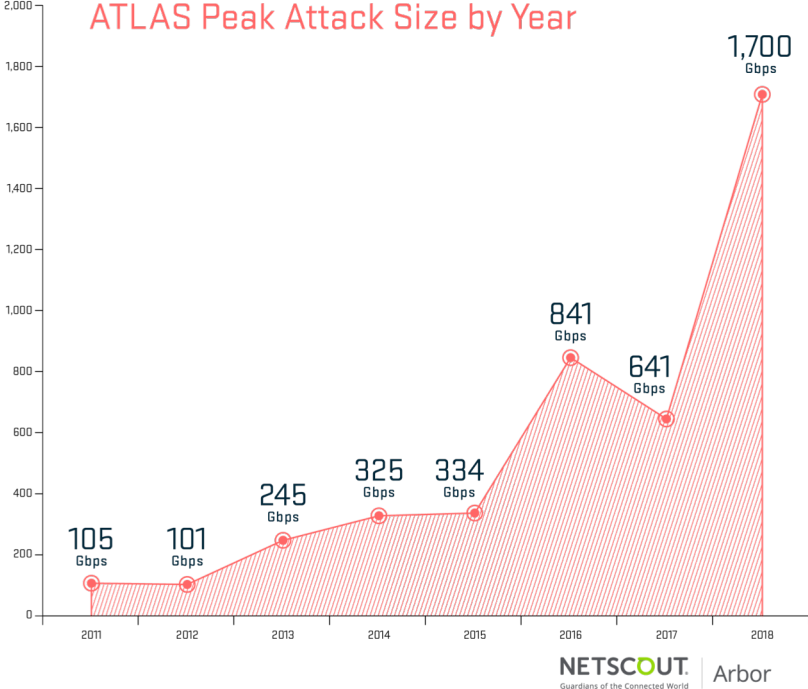
ATLAS Telemetry

- ATLAS observed 7.5 million DDoS attacks in 2017 vs. 6.8 million in 2016
- Largest attack in 2018 is 1.7 Tbps!
- Marked increase in the complexity of attacks

Number of DDoS Attacks 2016-2017



Source: NETSCOUT Arbor



NETSCOUT Arbor’s Active Threat Level Analysis System (ATLAS) delivers insight into 1/3 of global internet traffic

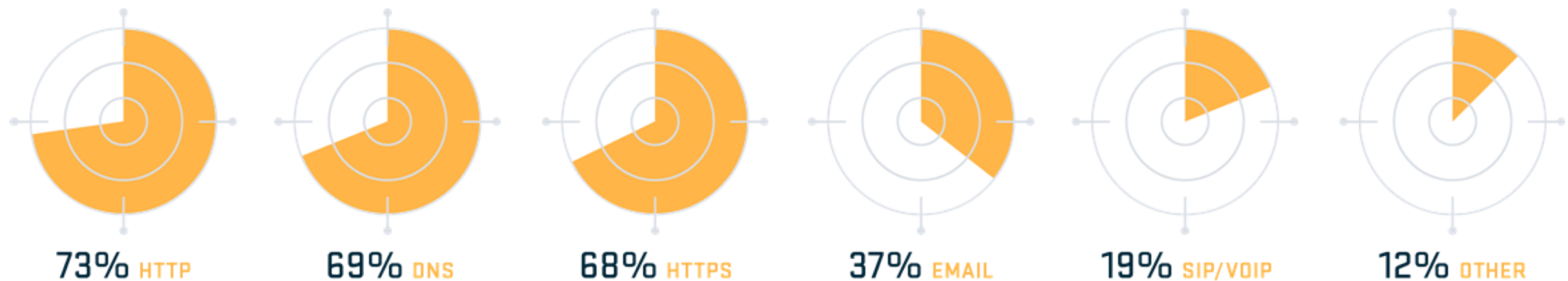


DDoS Continues to Evolve

Application-layer Attacks

- 30% increase of enterprises that experienced application-layer attacks in 2017
- Web services and DNS continue to dominate application-layer attacks

EGE Targets of Application-Layer Attacks



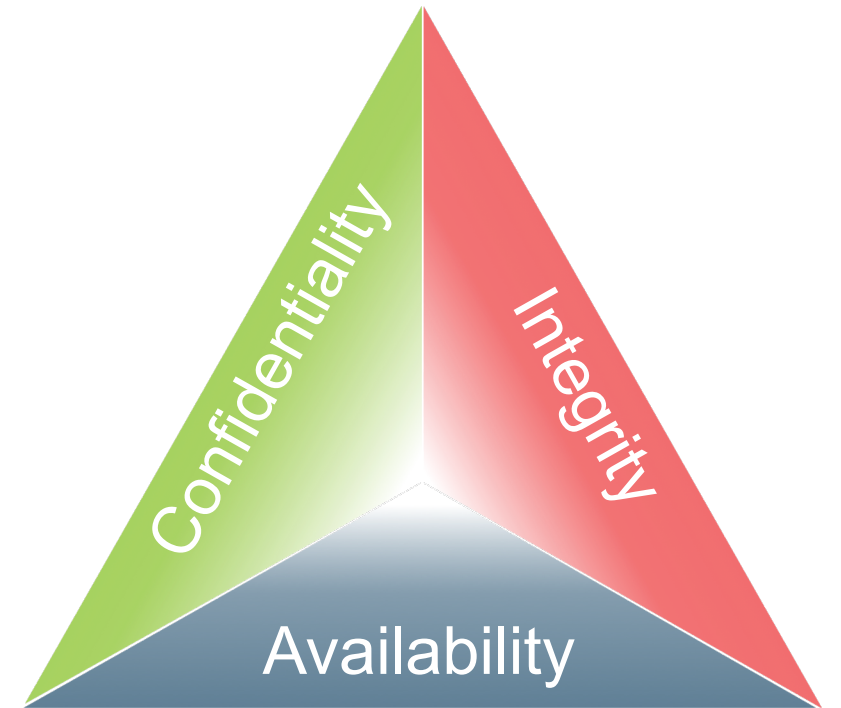
Source: NETSCOUT Arbor



A Statement on State

Firewalls, IPS devices and other security products effectively address network integrity and confidentiality, but fail to address **network availability**

- 61% of enterprises experienced attacks against infrastructure devices
- 51% had firewalls or IPS devices fail or contribute to an outage during a DDoS attack

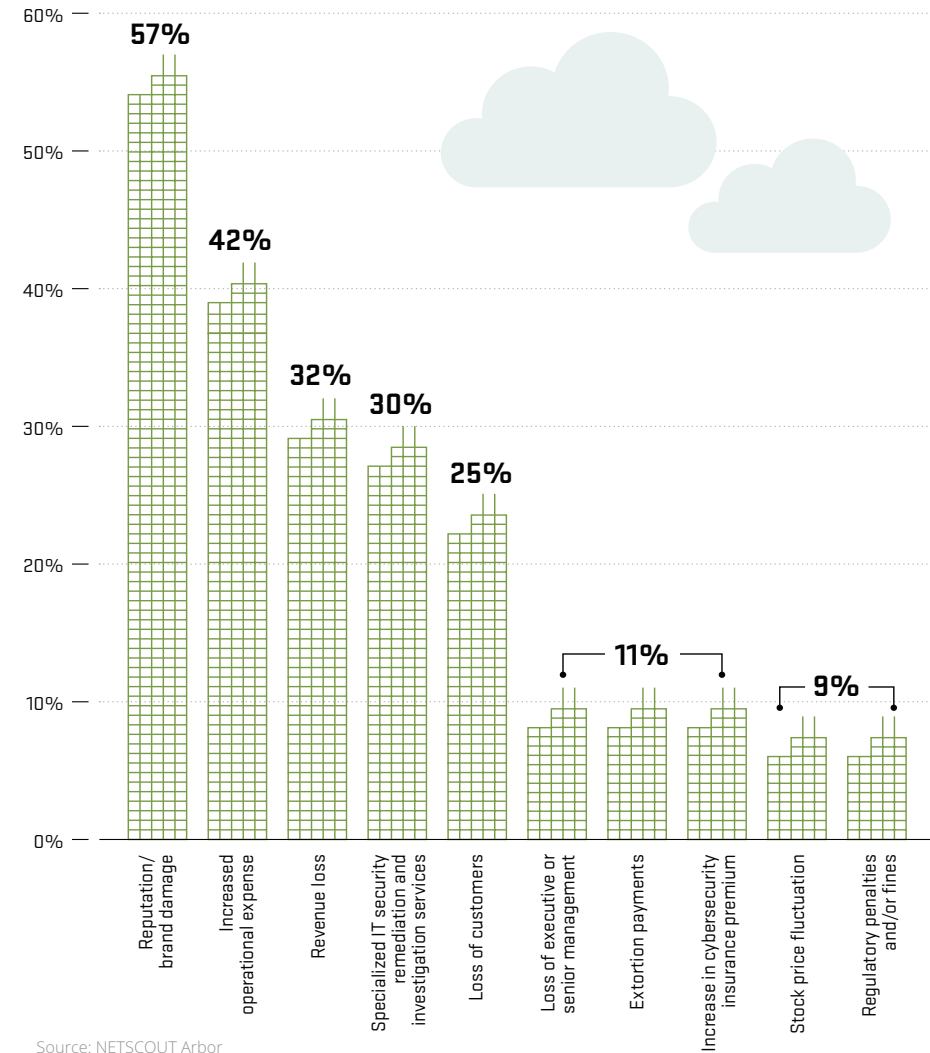


Consequences Are Rising for Enterprise

Drives Interest at C-Level

- Reputation / brand damage top business impact of an attack, operational expenses second
- 2X reporting revenue loss from DDoS attacks in 2017
- 77% report DDoS part of business or IT risk assessments
- 12% see costs of over \$100K, a 5x increase from last year

Business Impacts of DDoS Attacks



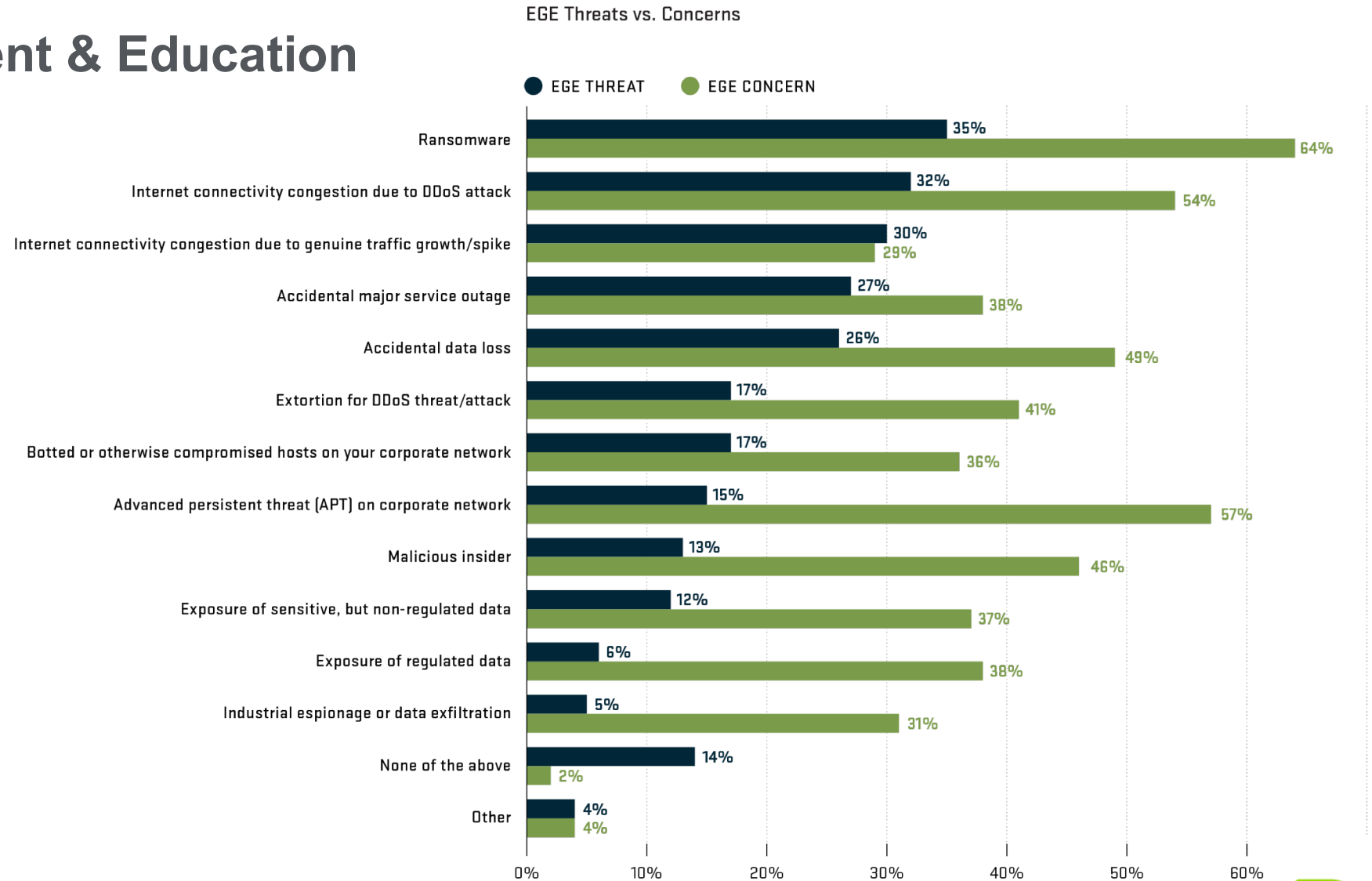
Source: NETSCOUT Arbor



Threats & Concerns

Enterprise, Government & Education

- Ransomware #1 threat and #1 concern
- DDoS #2 threat and #3 concern
- APT #2 concern, only experienced by 15%

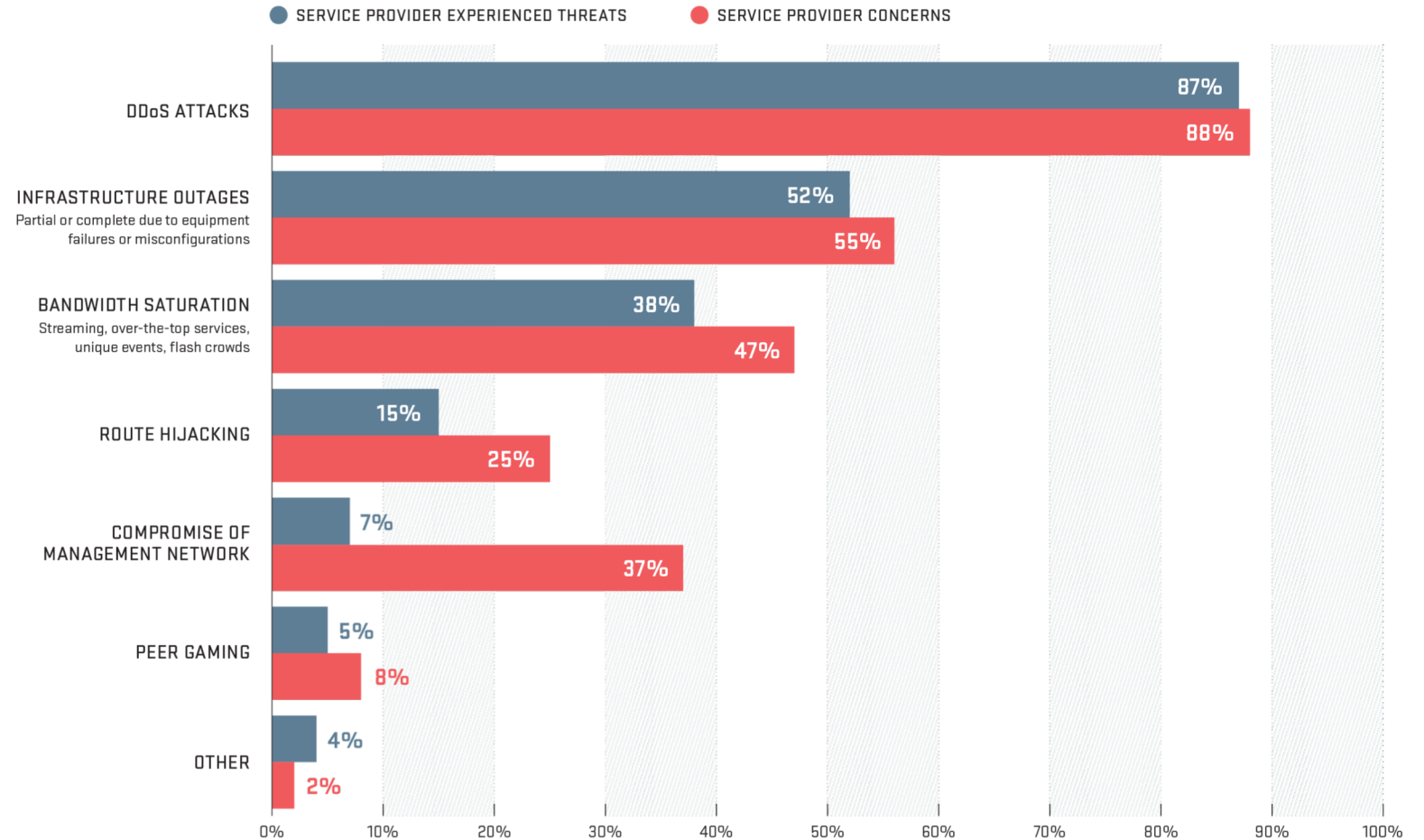


Threats & Concerns

Service Provider

- DDoS attacks represent top threat observed and equally concerning
- Infrastructure outages reclaims second spot
- Compromise of Mgmt. Networks is far concern than observed last year

Service Provider Experienced Threats and Concerns



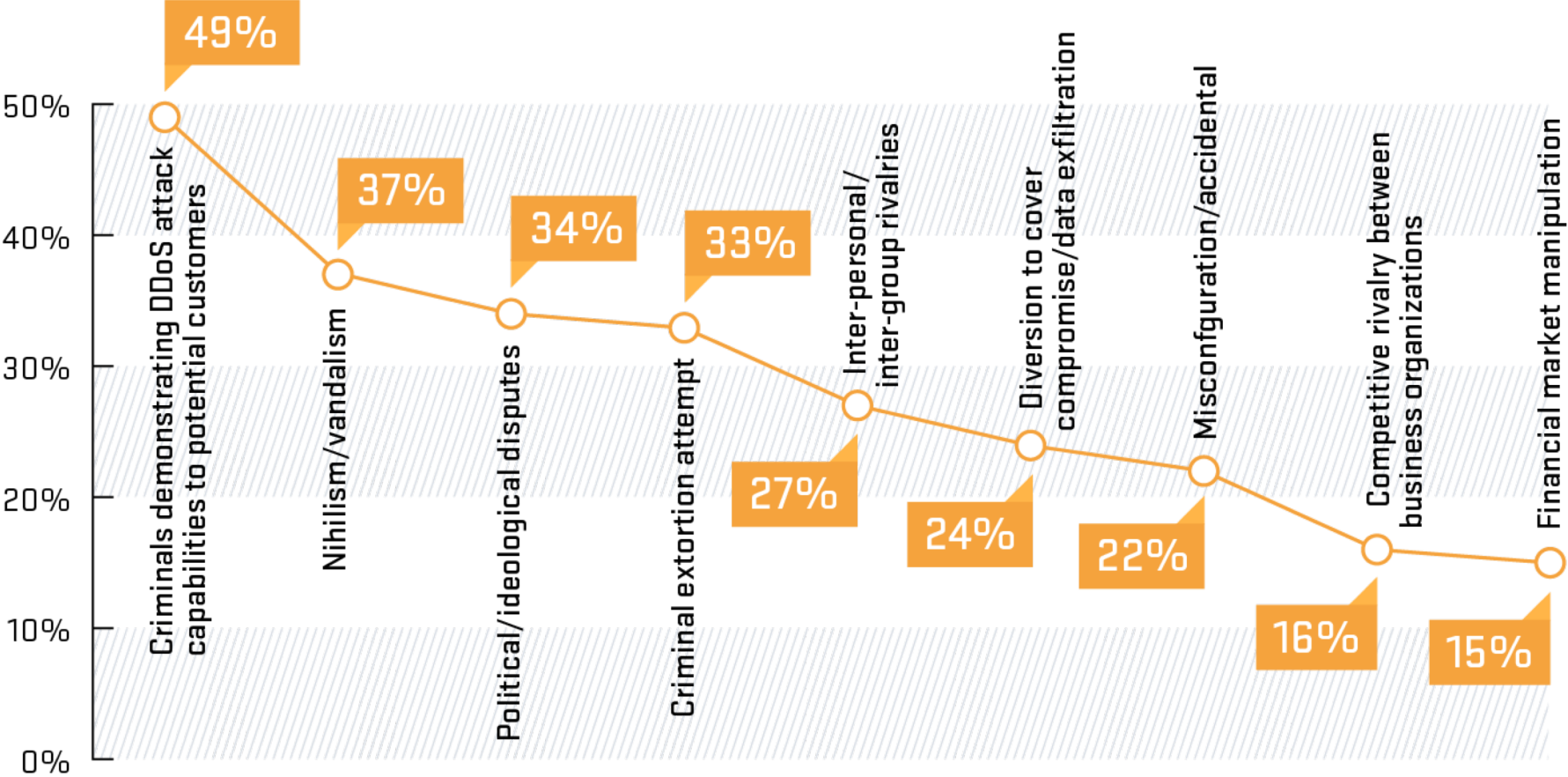
Source: NETSCOUT Arbor



Attack Motivations

Enterprise, Government, & Education

DDoS Attack Motivations



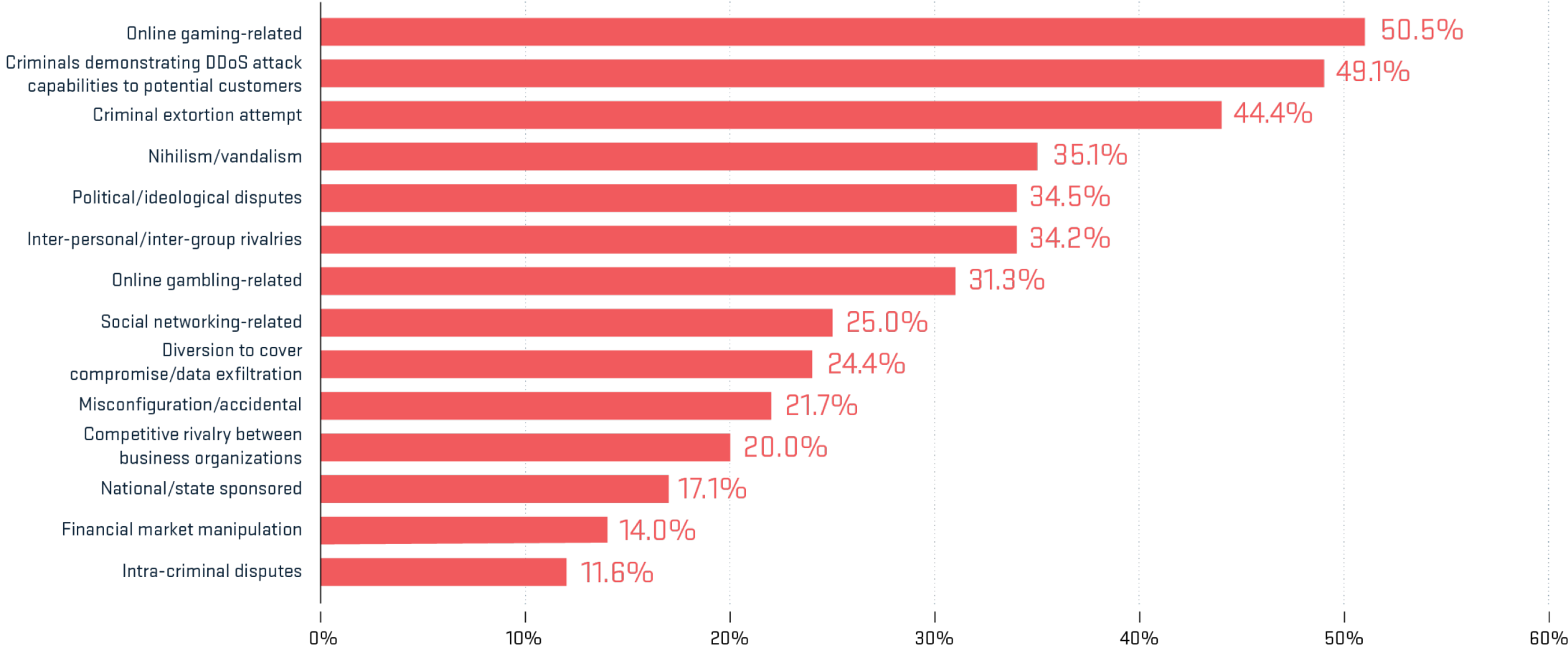
Source: NETSCOUT Arbor



Attack Motivations

Service Provider

Service Provider DDoS Attack Motivation

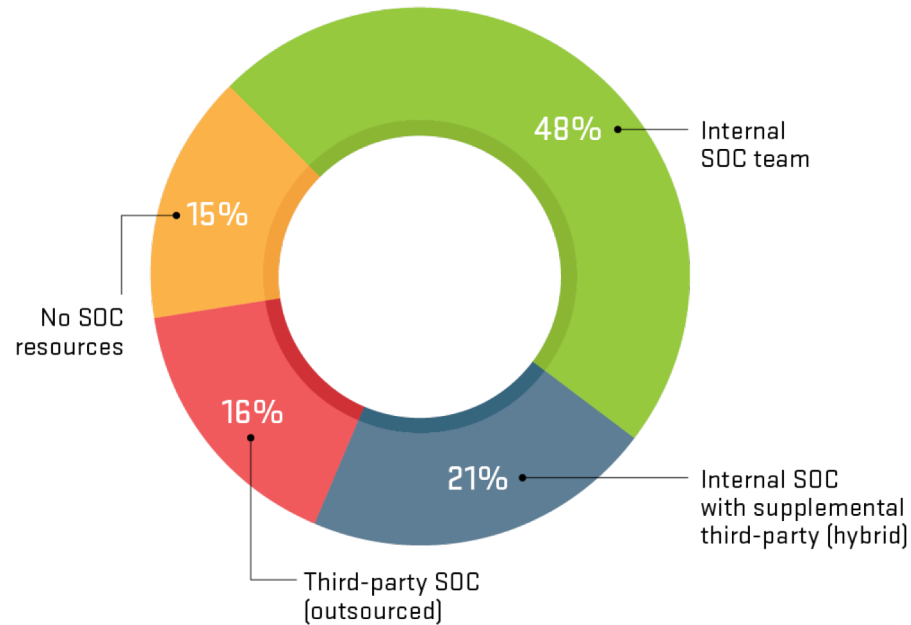


Source: NETSCOUT Arbor



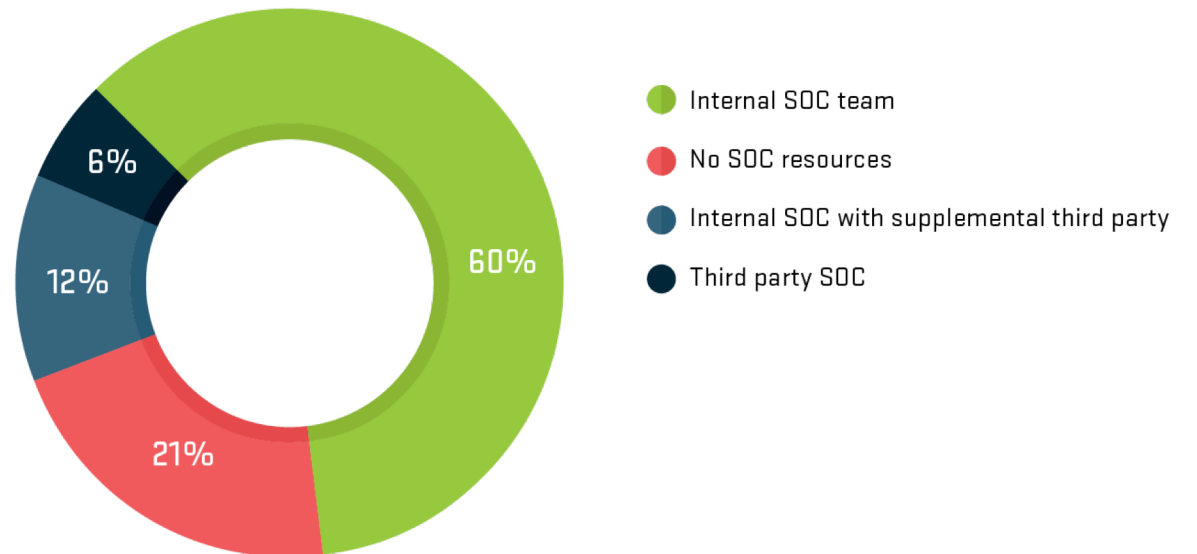
Operational Security

EGE Security Operations Center Resources



Source: NETSCOUT Arbor

SP Security Operations Center Resources



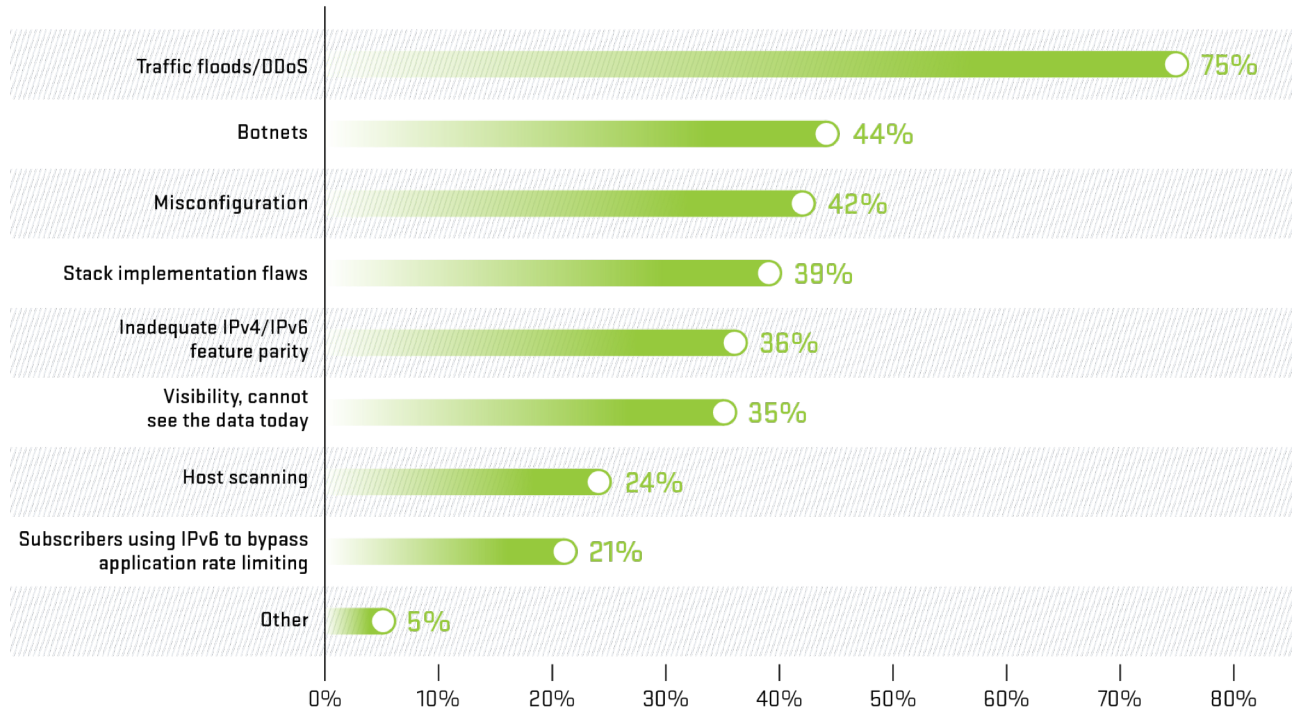
Source: NETSCOUT Arbor

- Lack of resources & difficulty hiring and retaining skilled personnel top concerns for building effective operational security team
- 23% of SP report security teams of 30+ vs. 14% of EGE



IPv6

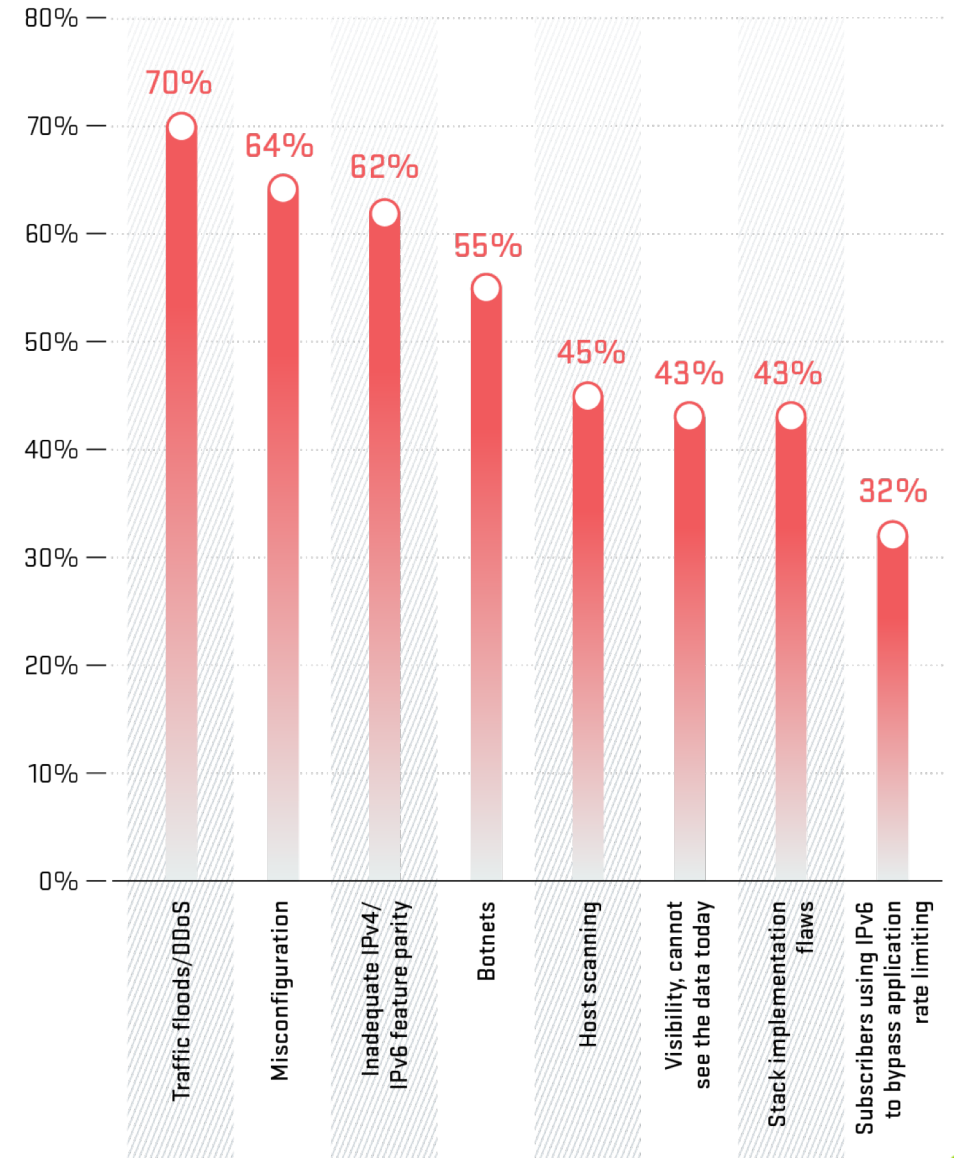
SP IPv6 Security Concerns



Source: NETSCOUT Arbor

- DDoS top concern
- Botnets and misconfiguration also top of mind

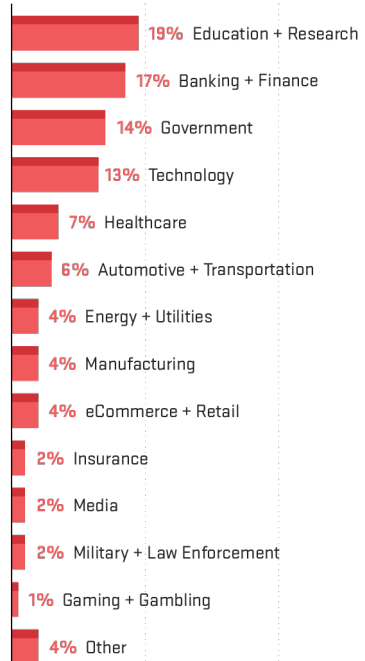
EGE IPv6 Security Concerns



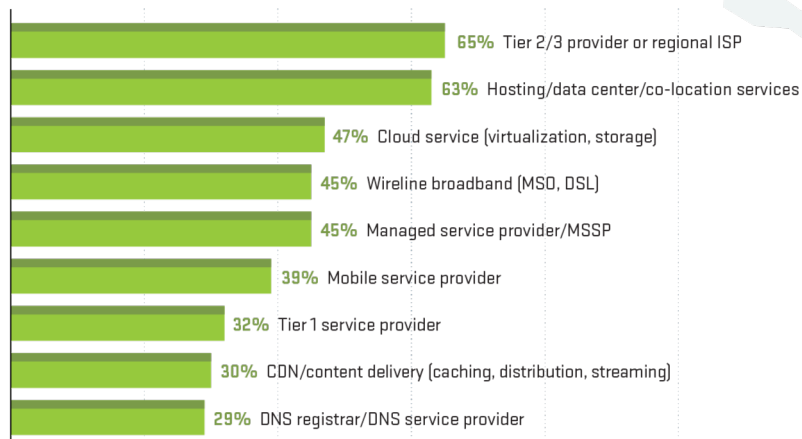
Source: NETSCOUT Arbor



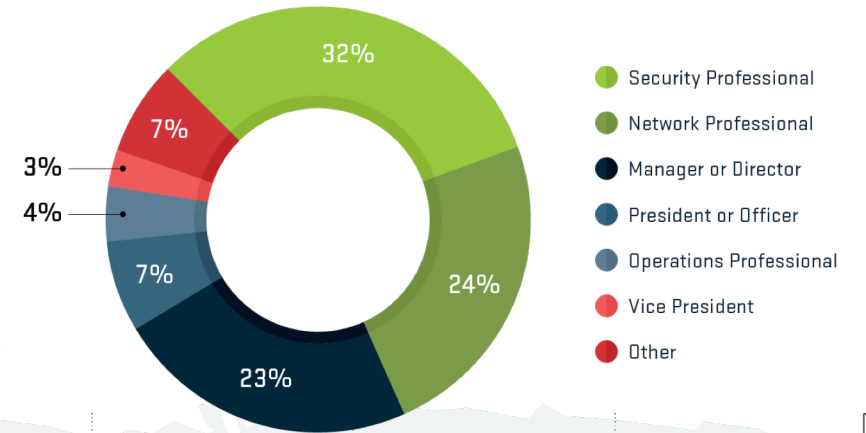
Survey Demographics



- 45% Enterprise Government & Education
- 55% Service Providers

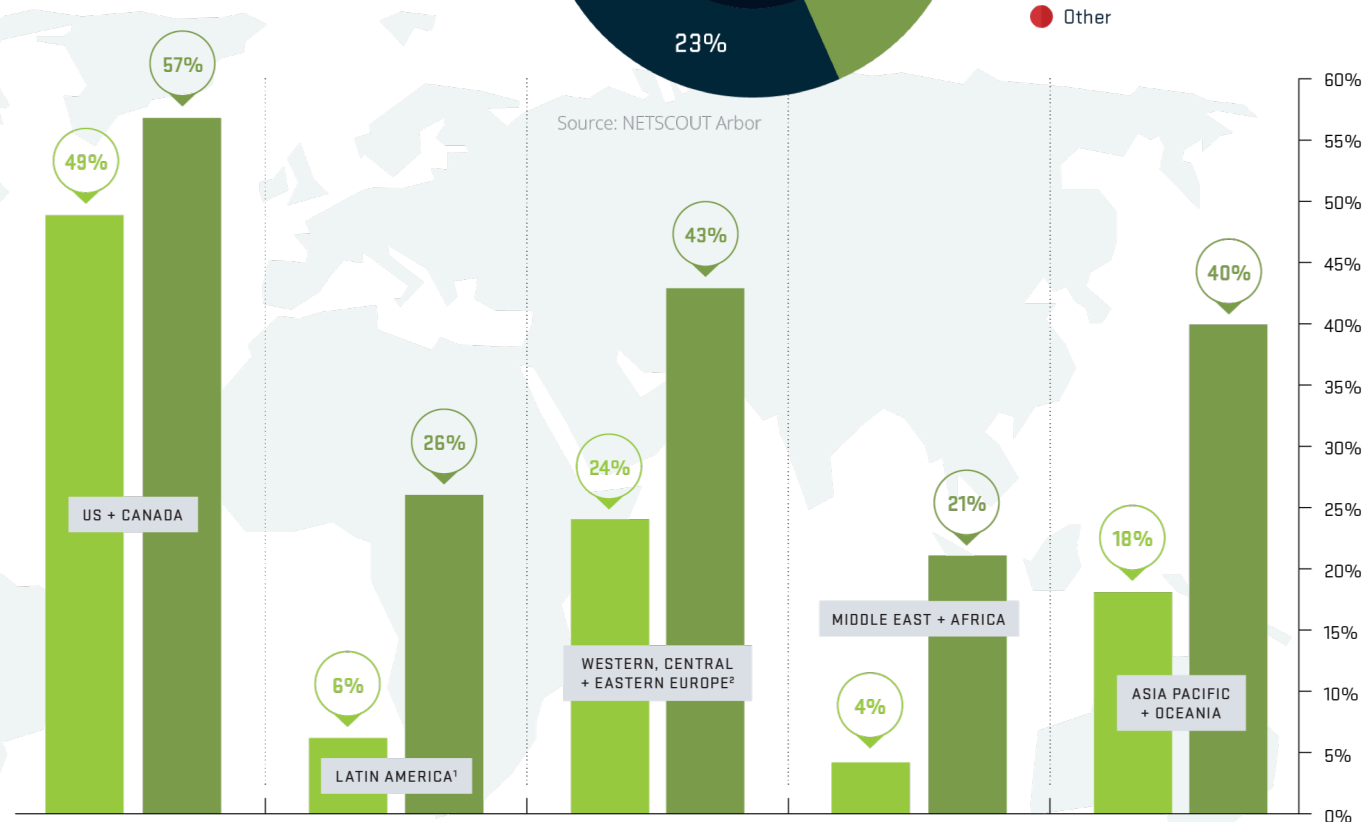


Respondent's Role in the Organization



Respondent's Geographic Information

- Where is your organization headquarters?
- In what region(s) of the world does your network operate?

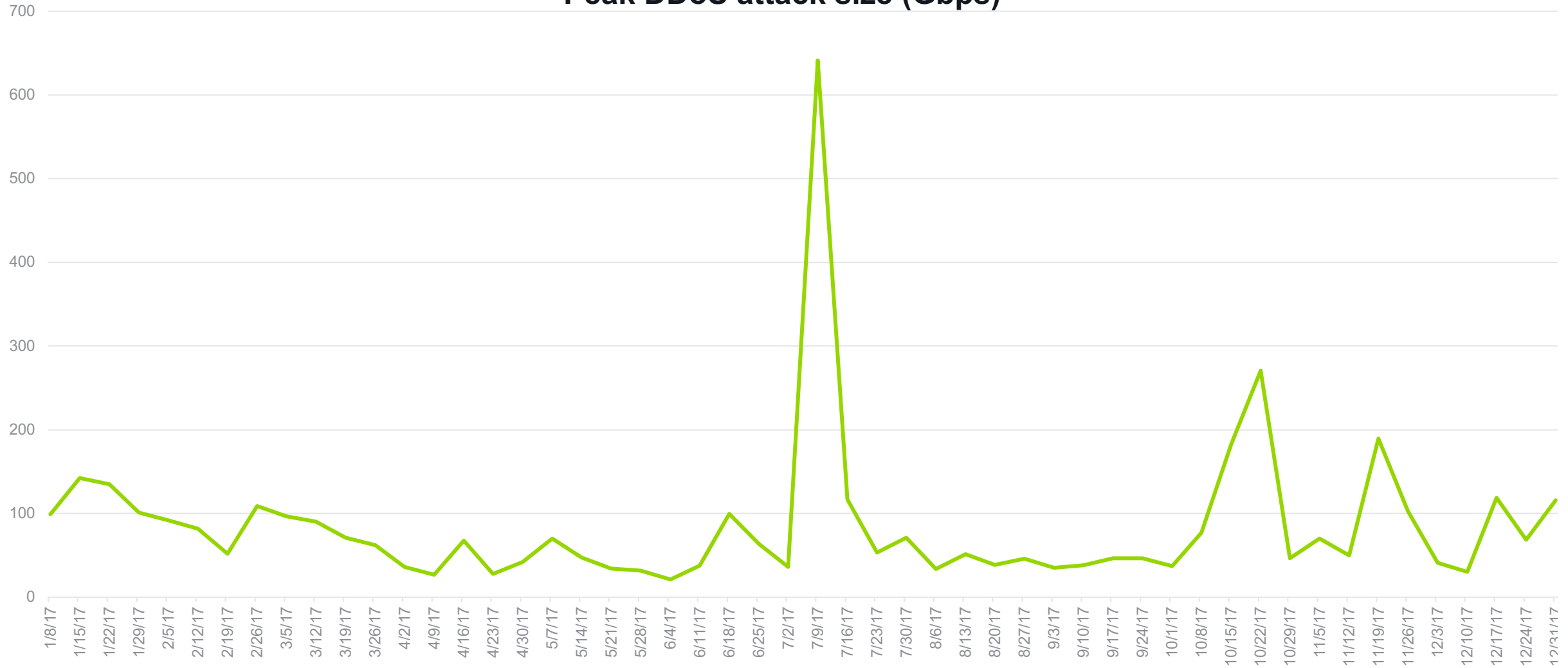


Source: NETSCOUT Arbor



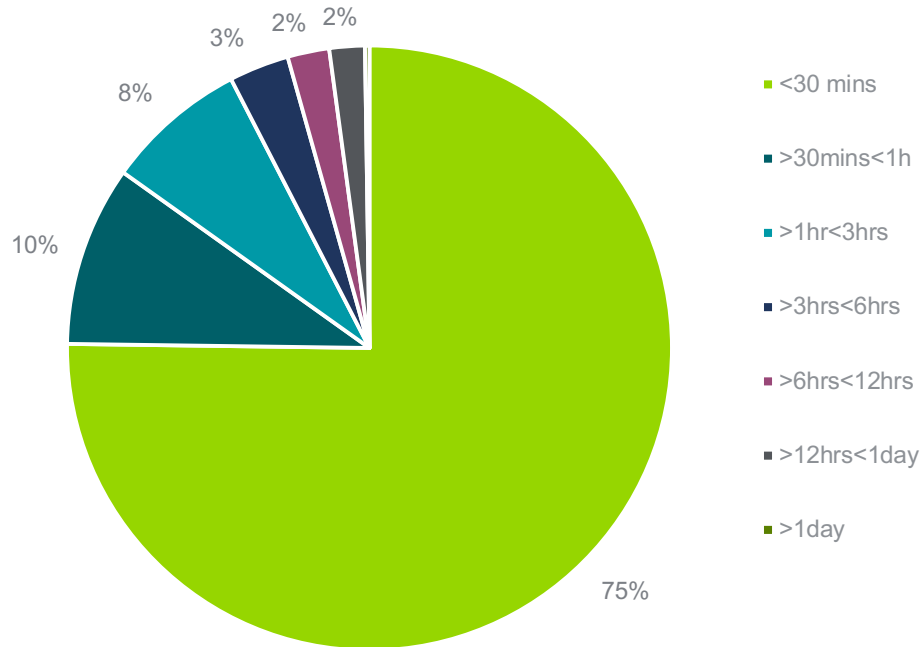
LATAM DDoS 2017

Peak DDoS attack size (Gbps)

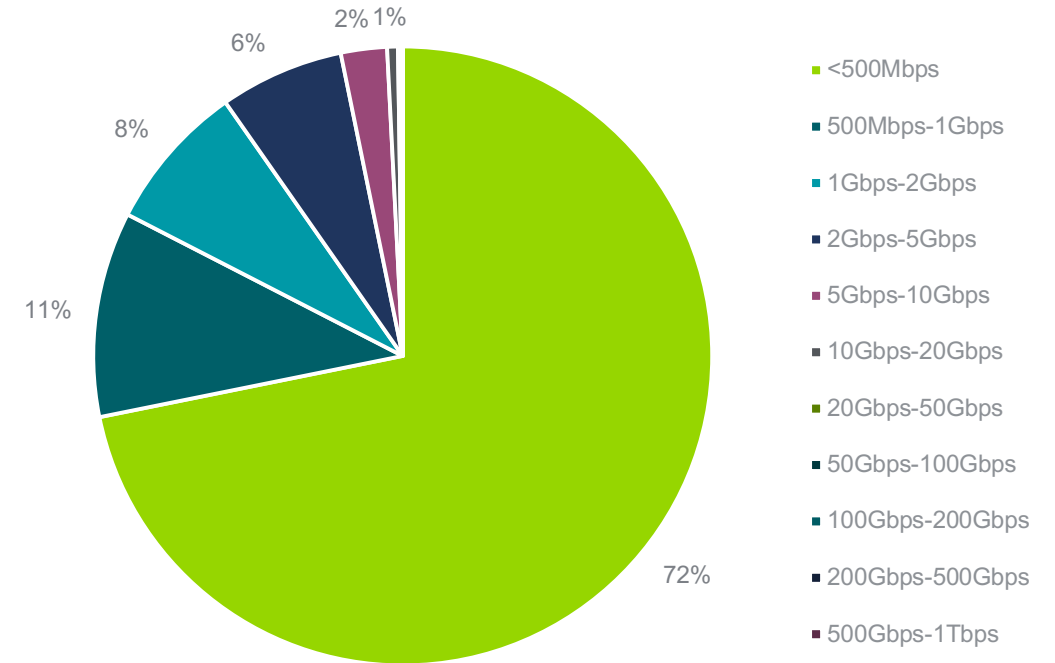


LATAM DDoS 2017

DDoS attack duration

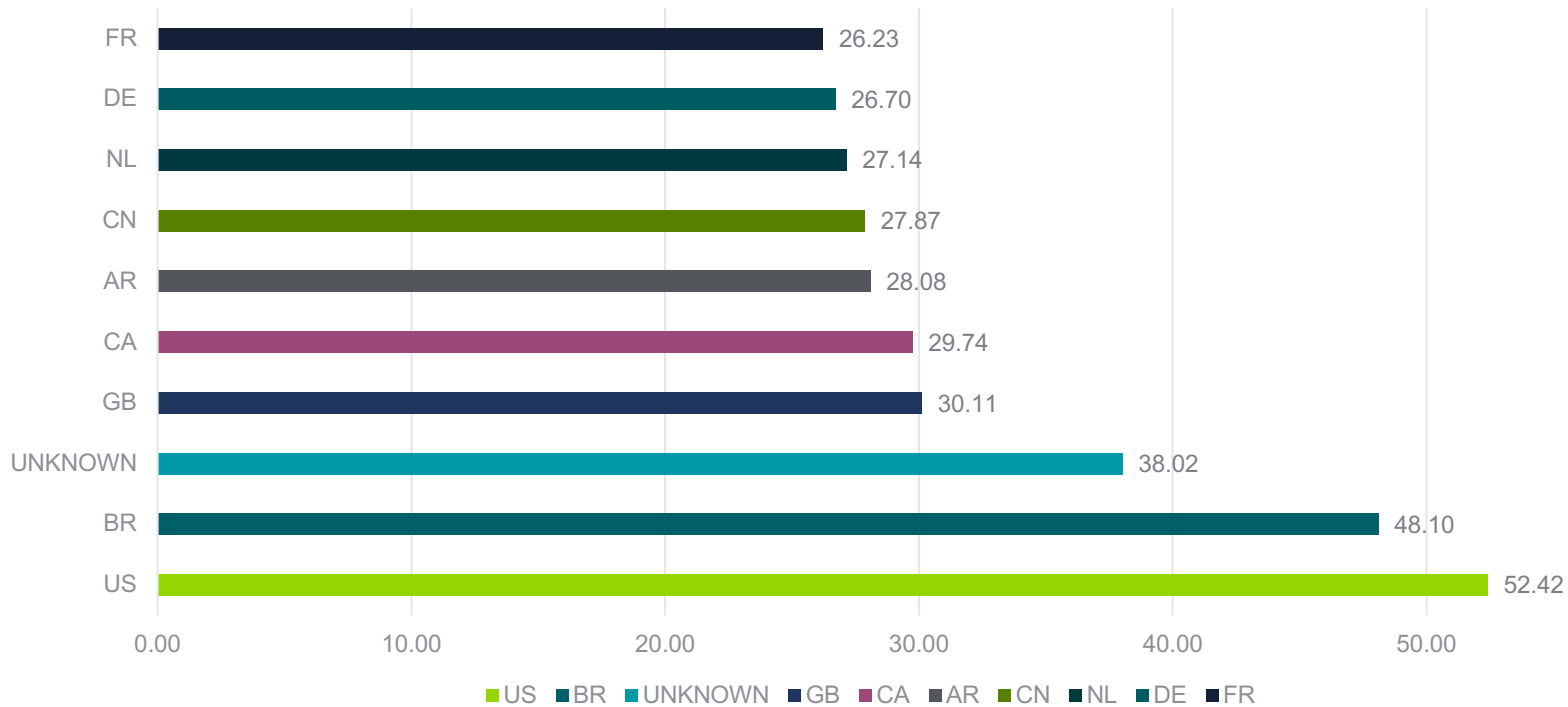


DDoS attack size (bps)

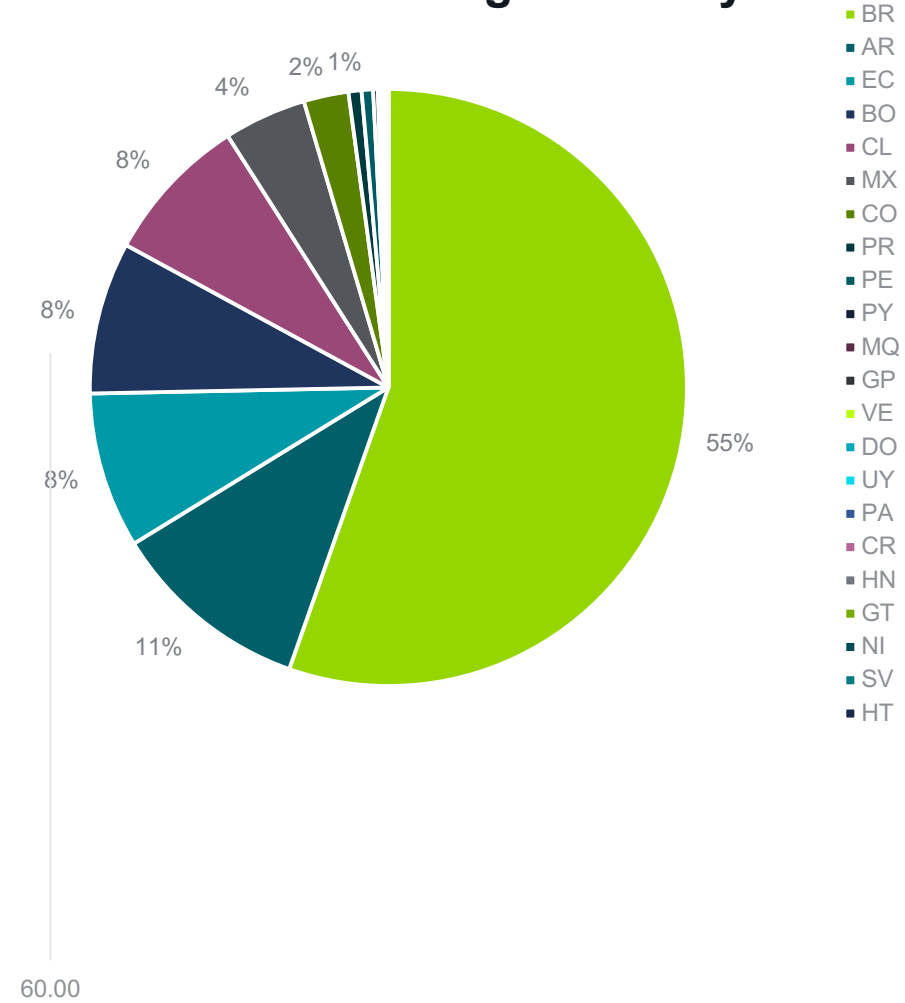


LATAM DDoS 2017

DDoS attack source country (%)



DDoS attack target country



Thank You.

Contact: kleber@arbor.net

www.netscout.com