Ordine degli Ingegneri della Provincia di Roma

Attacchi informatici:
Strategie e tecniche per capire, prevenire e proteggersi dagli attacchi della rete

Analisi degli attacchi DDOS e delle contromisure

Alessandro Tagliarino

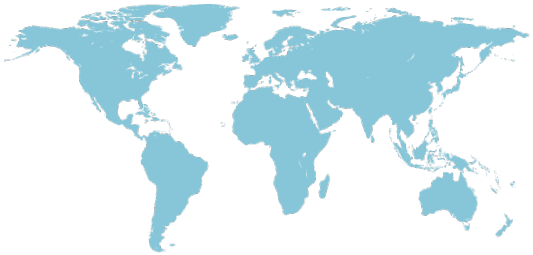
06 Novembre 2017

WHO IS ARBOR NETWORKS?

Arbor market position in Carrier, Enterprise and Mobile DDoS equipment market segments

17

Number of years Arbor has been delivering innovative security and network visibility technologies & products



> 110

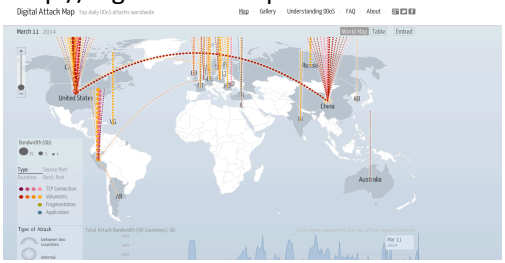
Number of countries with Arbor products deployed

100%

Percentage of world's Tier 1 service providers who are Arbor customers

Amount of global traffic monitored by the ATLAS security intelligence initiative right now!

http://Digitalattackmap.com



Overview

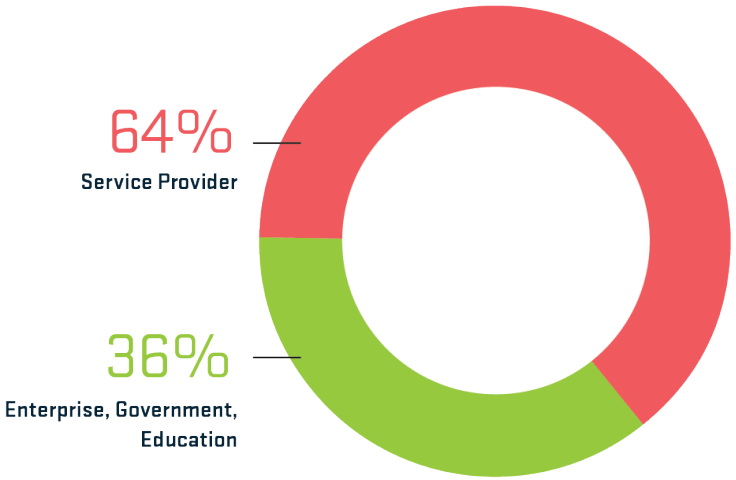
This presentation provides a summary of the results of Arbor Networks' 12th annual Worldwide Infrastructure Security Report (WISR)

The WISR documents the collective experiences, observations and concerns of the operational security community in 2016 plus forecasts for the coming year

The WISR has changed immeasurably in terms of its scope and scale over 12 years, but the core goal is still to provide real insight into infrastructure security from an operational perspective

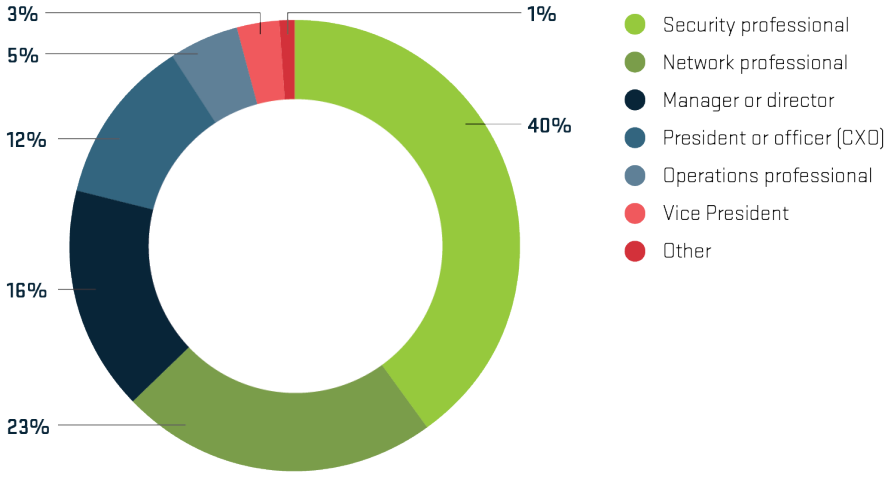
Survey Demographics

Respondent Classification



Source: Arbor Networks, Inc.

Respondent's Role in the Organization



Source: Arbor Networks, Inc.

- SP respondents : 51% Tier 2/3 operators & 25% Tier 1
- EGE respondent : 61% enterprise, 35 % education & 14% government
  - Enterprise: 32% banking/ finance up from 18% last year.
  - Technology, automotive/transportation and manufacturing are also well represented, rounding out the top 4
- Geographic Split: 32% North America, 28% Europe, 23% APAC, 10% Middle East/Africa & 7% LATAM

Things You Should Know About DDoS Attacks

- Its never been easier to launch a DDoS attack.
- DDoS attacks are increasing in size, frequency and complexity.
- DDoS attacks are used as smoke screens or forms of diversion during advanced threat campaigns[2].
- One Of the Top 3 causes of unplanned outages, DDoS attacks are the most costly to an organization[3]

Did You Know?

$5:$100sK

DDoS for Hire

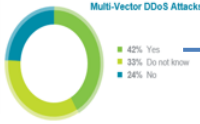
For $5/hr anyone can launch a DDoS attack an cause $100sK in damage

800Gbps

…DDoS attack size increasing [1]

74%

…involved DDOS as a diversion[2]



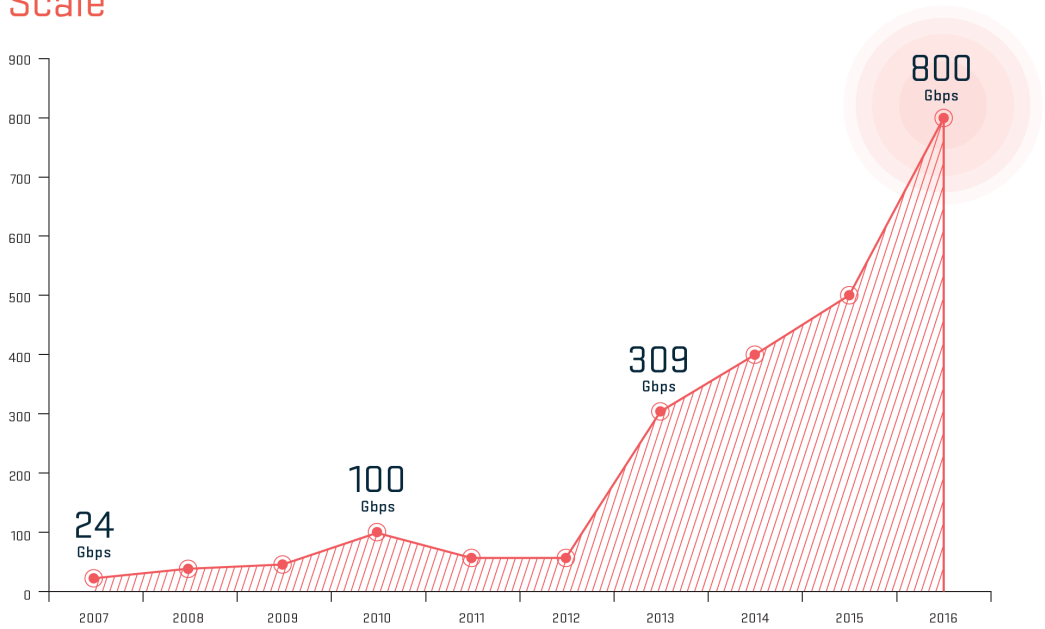
42%

…experienced multi-vectored attacks[1]

78%

…Increase in demand for DDoS Protection services[1]

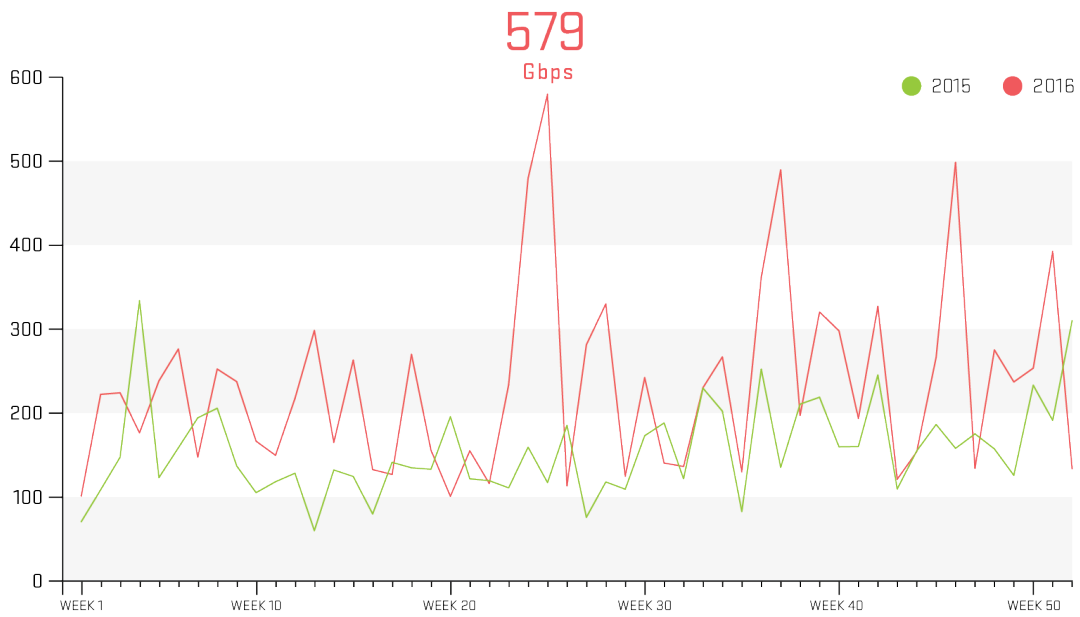
Scale : Volumetric Attacks Increase



- 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
- 41% of EGE respondents and 61% of data-center operators reported attacks exceeding their total Internet capacity

Scale : The ATLAS Perspective

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



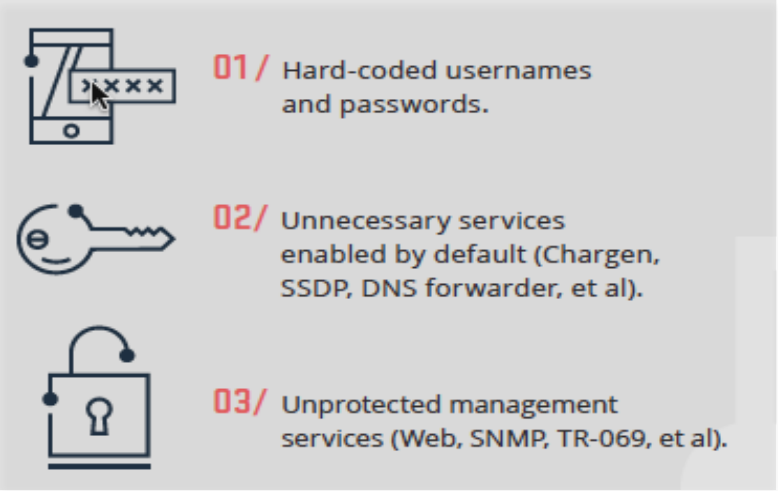
Source: Arbor Networks, Inc.

- 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

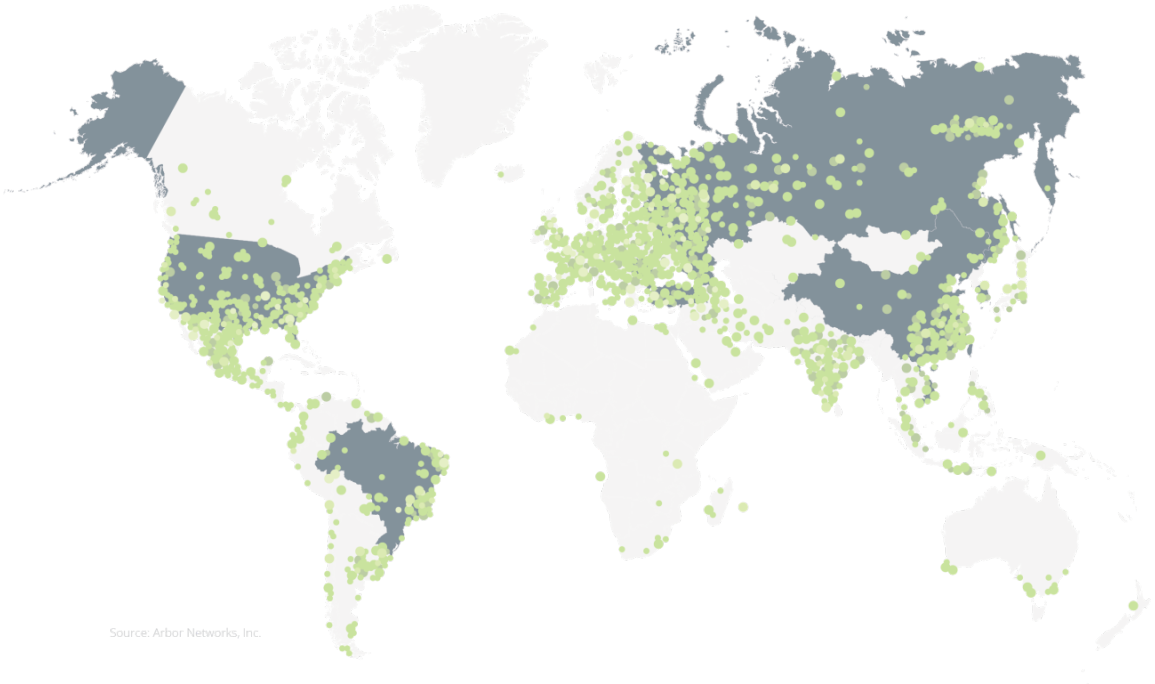


The Result

- 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 the Olympics, 620Gbps against Krebs, Dyn etc..

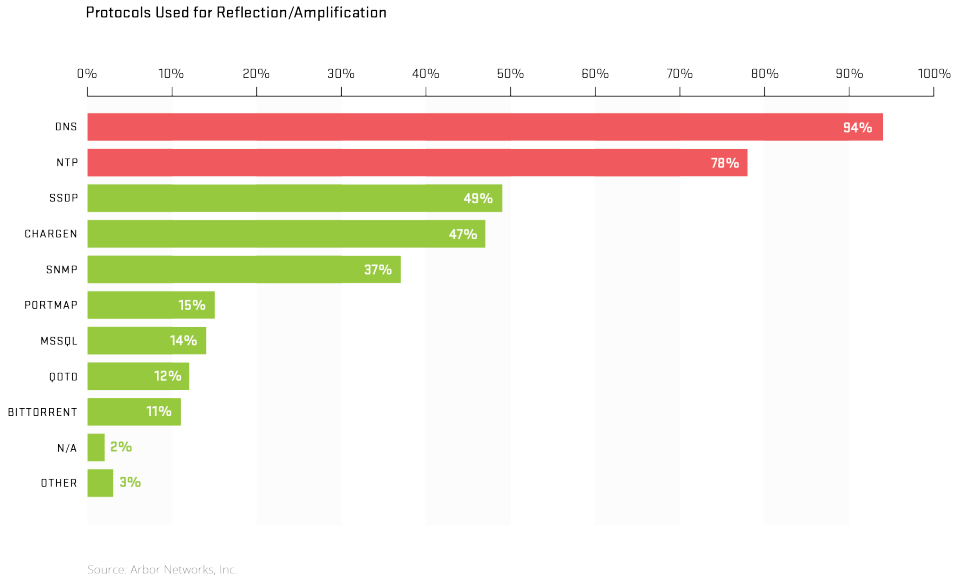
Scale: Driving Factors, Mirai

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

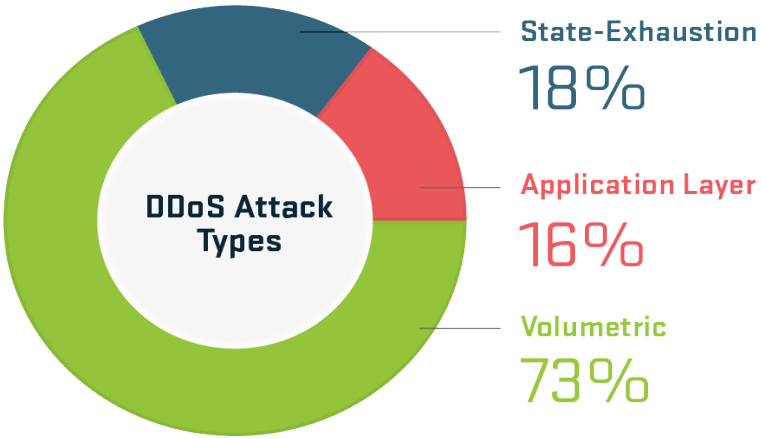
Scale: Driving Factors, Reflection Amplification



- 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

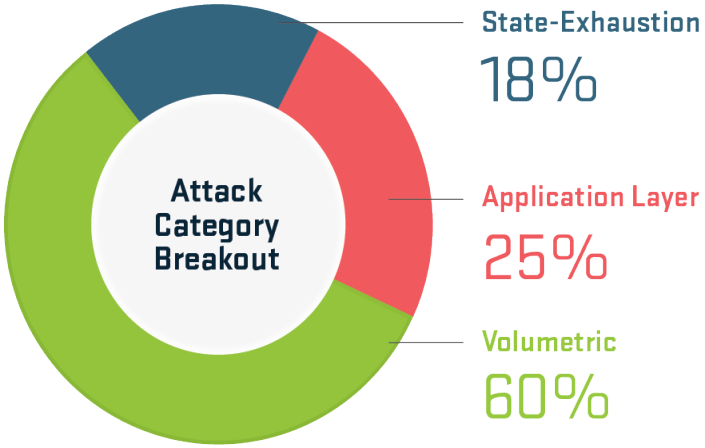
Complexity : Attack Types

Service Provider Attack Types



Source: Arbor Networks, Inc.

EGE Attack Types

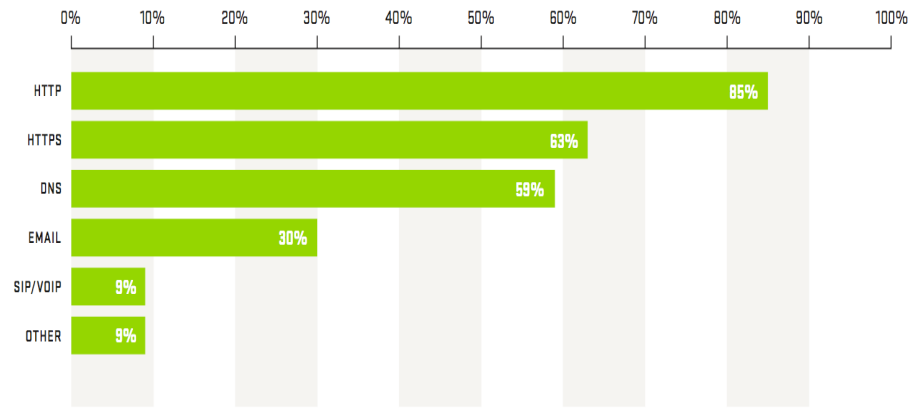


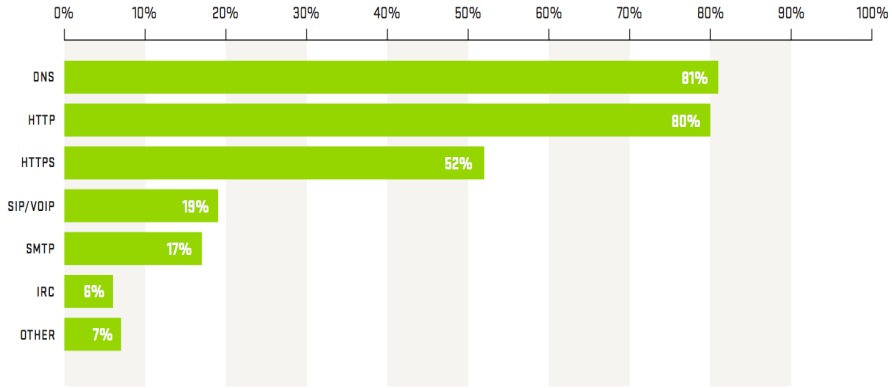
Source: Arbor Networks, Inc.

- 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

EGE Service Targets



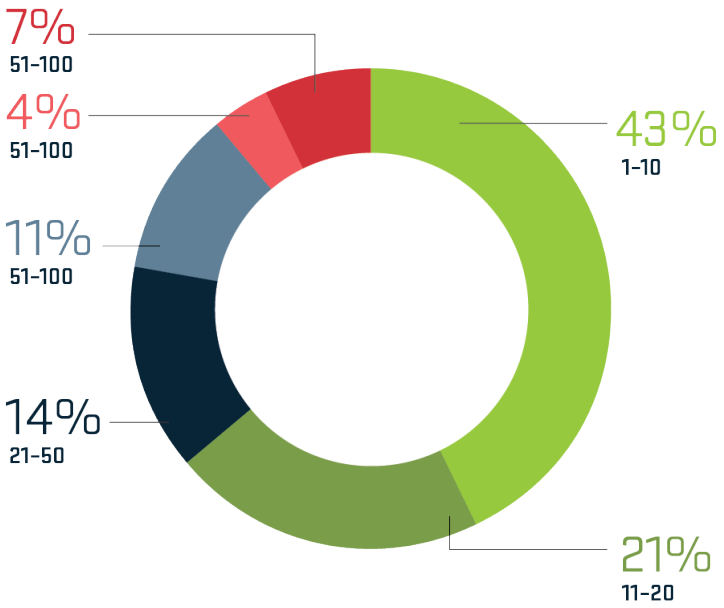


SP Service Targets

- DNS and HTTP the most common services targeted by application layer 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

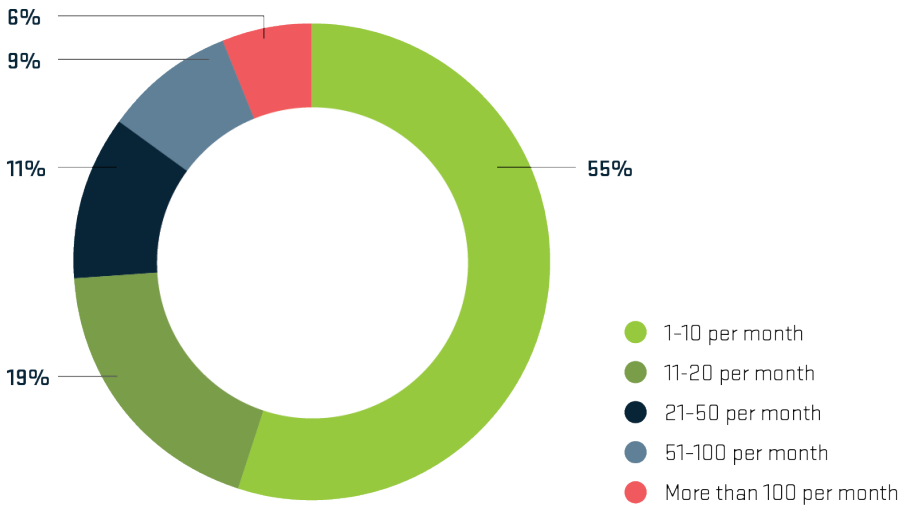
Frequency : Up Across the Board

Data Center DDoS Attack Frequency



Source: Arbor Networks, Inc.

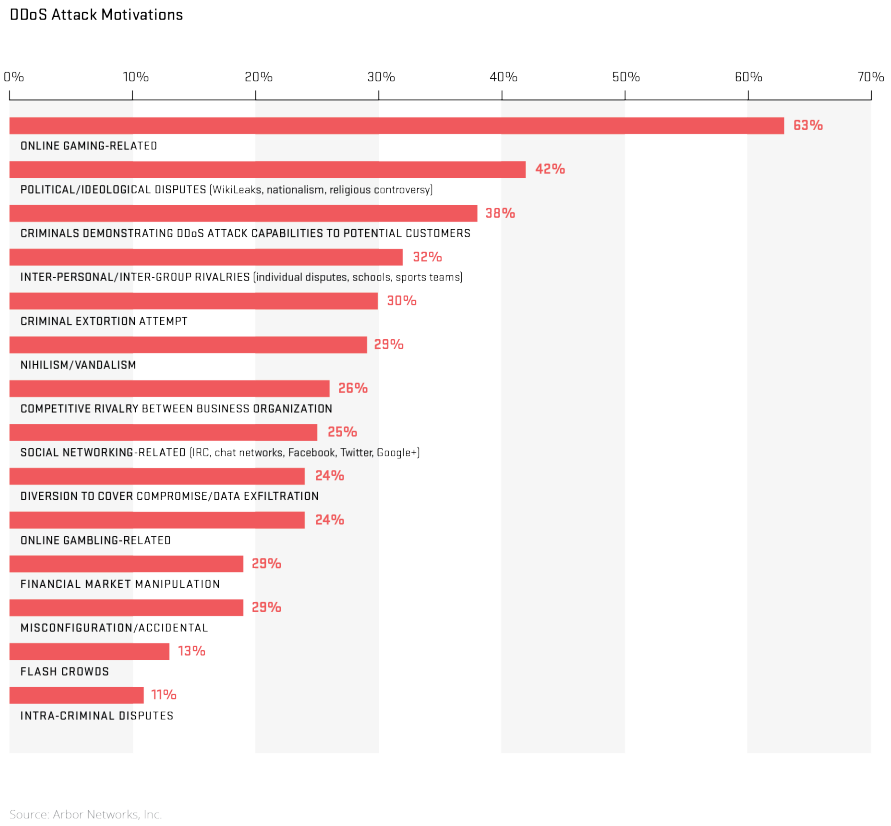
EGE DDoS Attack Frequency Per Month



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.

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%

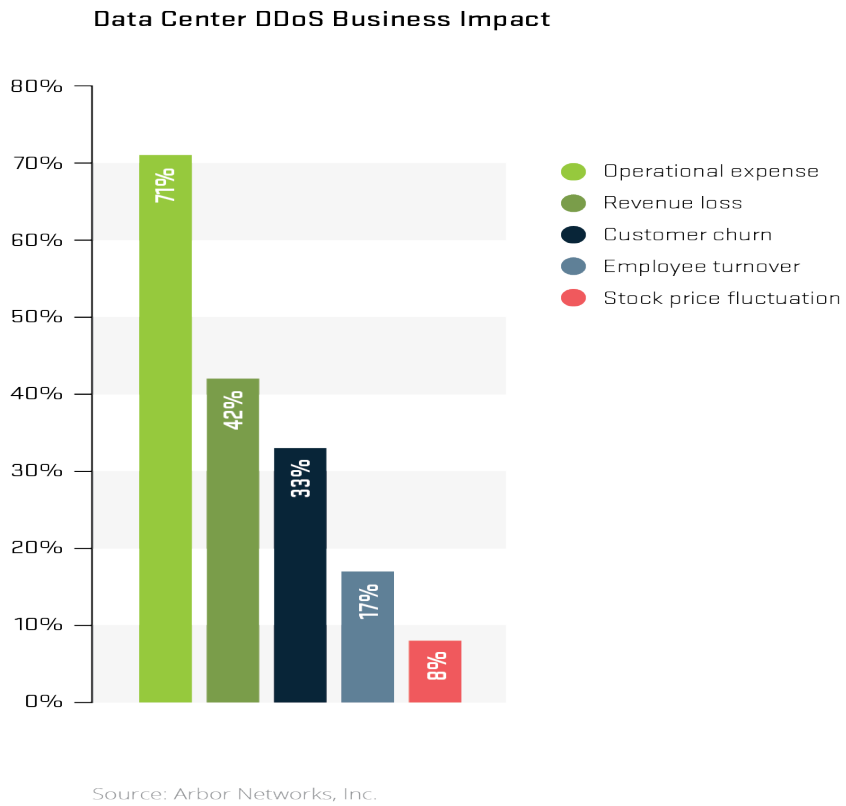
Impact : Targets

- SPs see Government, Finance and Hosting as top targets
- SPs seeing attacks on cloud services drops from one third to one quarter
- 42% of EGE respondents experienced an attack
  - 63% of finance, up from 45%
  - 53% of government, up from 43%

Attack Target Customer Verticals

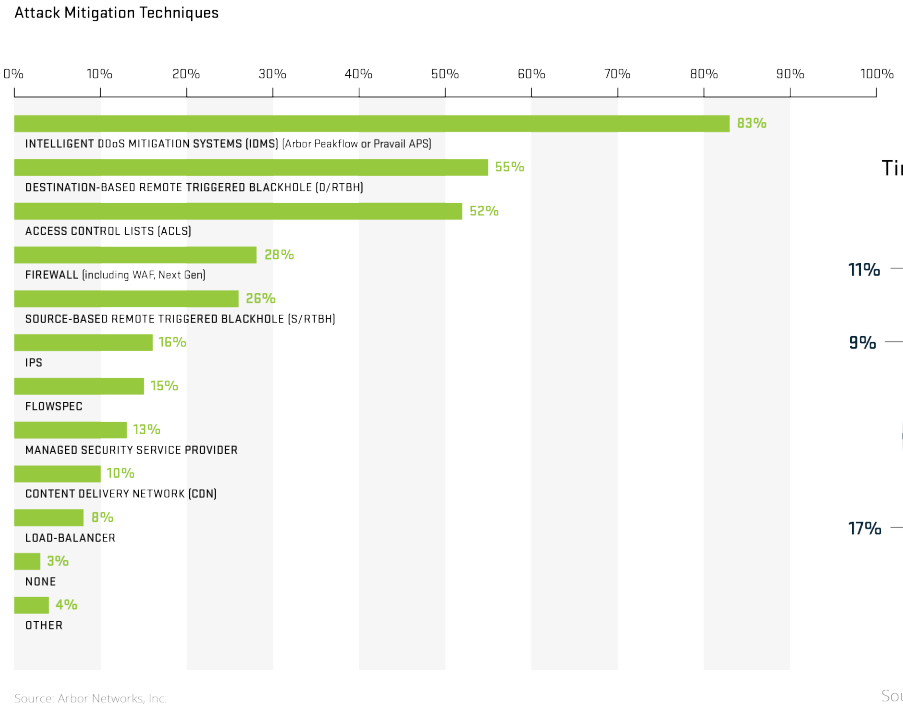
Source: Arbor Networks, Inc.

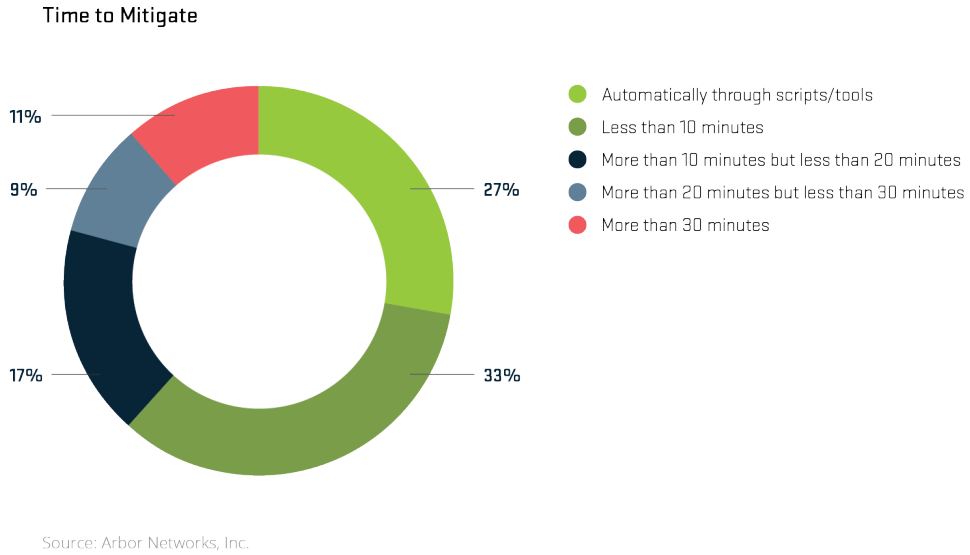
Impact : Data Center



- Nearly three quarters of data center respondents saw between 1 and 20 attacks that impacted their service in 2016
- Operational expenses are top business impact
- Significant increase in revenue loss, up from 33% to 42%
- 23% estimate cost of a significant attack over $100K, 5% estimate over $1M

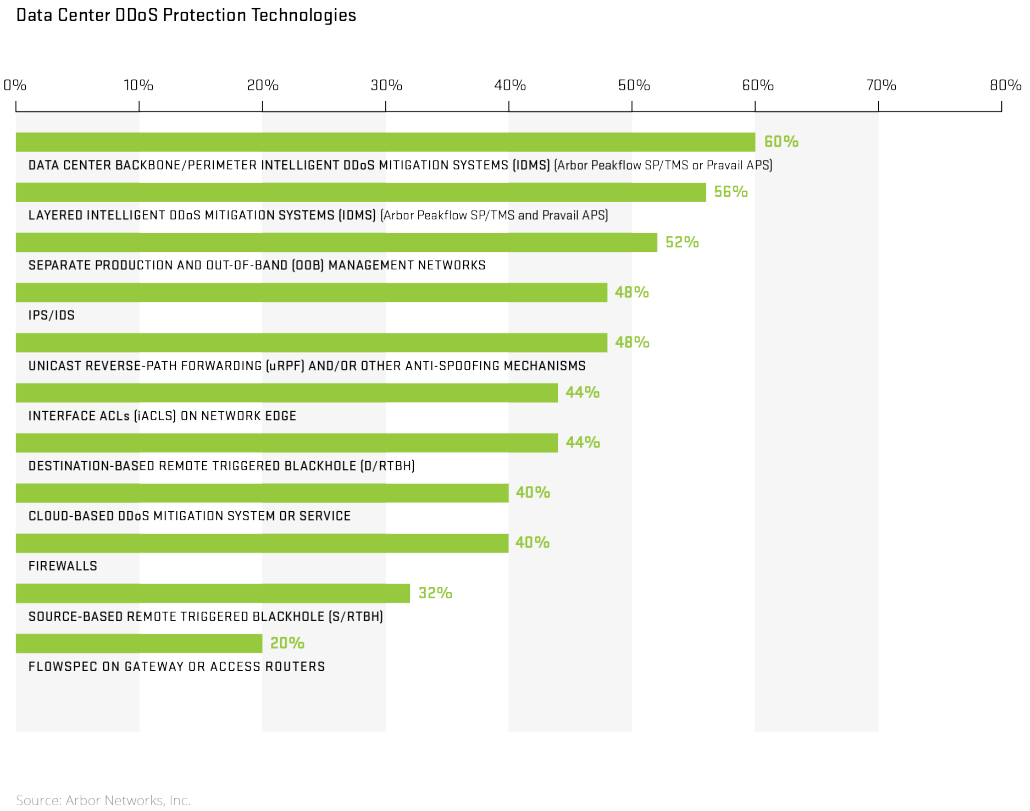
Mitigation : SPs Continue to Impress





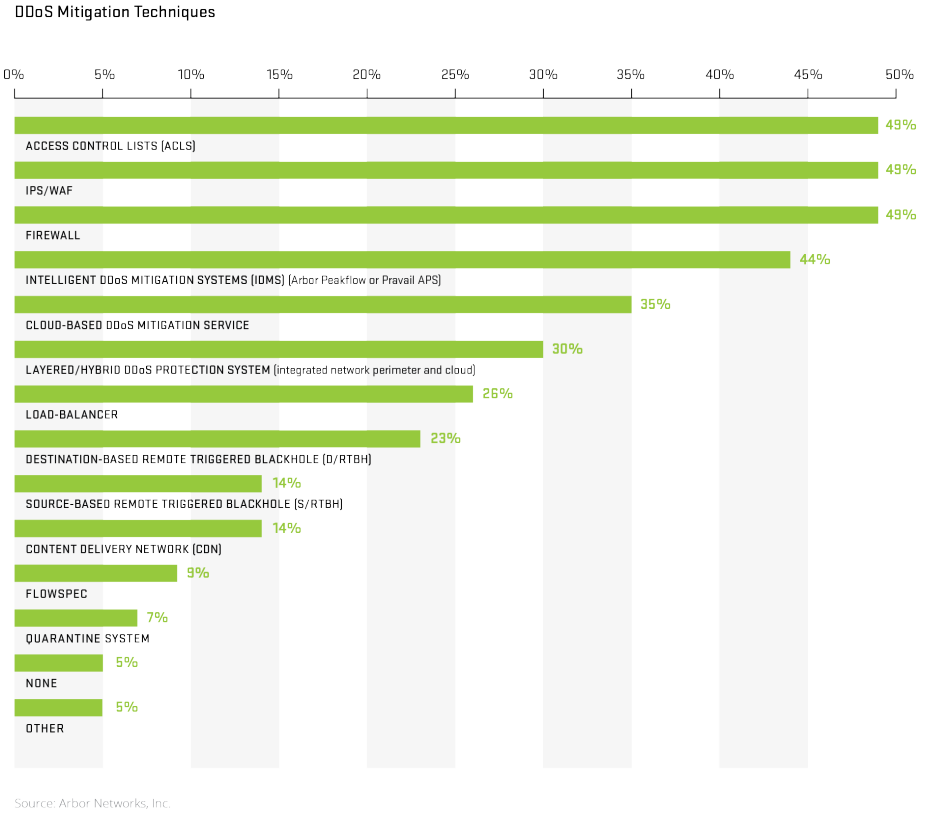
- 83% of SPs use IDMS to mitigate DDoS attacks
  - Use of IDMS and D/RTBH are both increasing
- 77% of SPs mitigate attack in less than 20 minutes
  - 27% mitigate automatically
- 78% of SPs see more demand from customers, up 4 percent over last year
  - Government, Finance, eCommerce and Hosting are driving demand

Mitigation : Data Center Improves



- 60% use IDMS
- 40% use firewalls
  - down from 71%

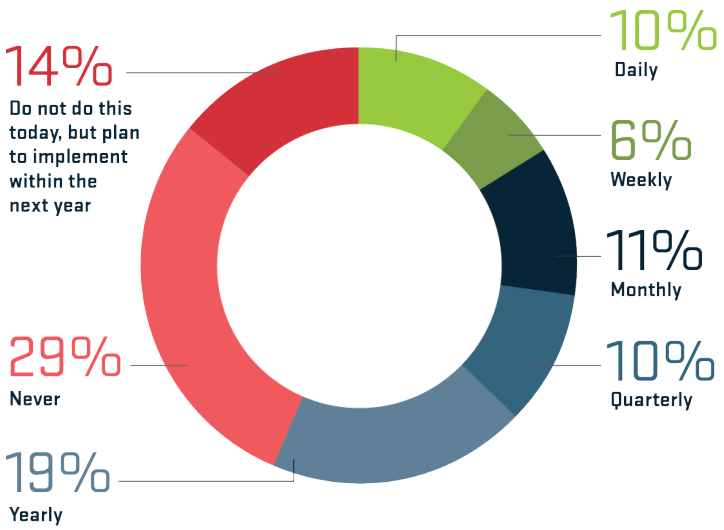
Mitigation : EGE Improves



- Firewalls, IPS/WAF and ACLs most common
- 35% use cloud DDoS mitigation
  - Up from 28%
- 30% use layered DDoS mitigation
  - Up from 23%

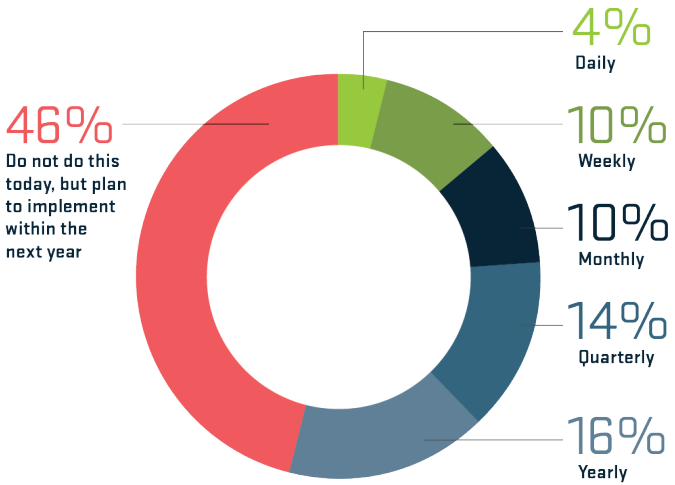
SP Organizational Security

DDoS Simulations



Source: Arbor Networks, Inc.

EGE DDoS Simulations



Source: Arbor Networks, Inc.

- Nearly half of SPs now implement anti-spoofing filters
- Rehearsing DDoS attack processes and procedures is key
  - 10% increase in SPs running simulations, 37% do this quarterly
  - EGE 55% now run simulations, 40% do this quarterly
- Difficulty in hiring and retaining personnel remains a key issue for both SP and EGE respondents

Q&A