WORLDWIDE INFRASTRUCTURE SECURITY REPORT

11th Annual WISR Overview – LACNIC / LACSEC

Carlos Ayala

cayala@arbor.net

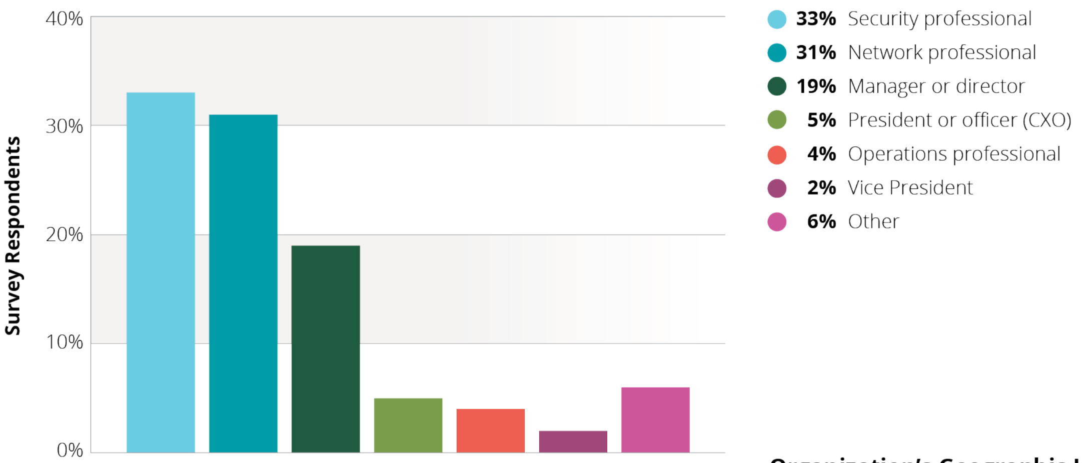
ARBOR®
NETWORKS

AGENDA

- Demographics
- Advanced Threats
- Incident Response
- Incident Response Improvement
- DDoS
- DDoS complexity
- DDoS reflection amplification
- DDoS motivations
- DDoS business impact
- DNS services
- Organizational security

SURVEY DEMOGRAPHICS

Respondent's Role in Organization

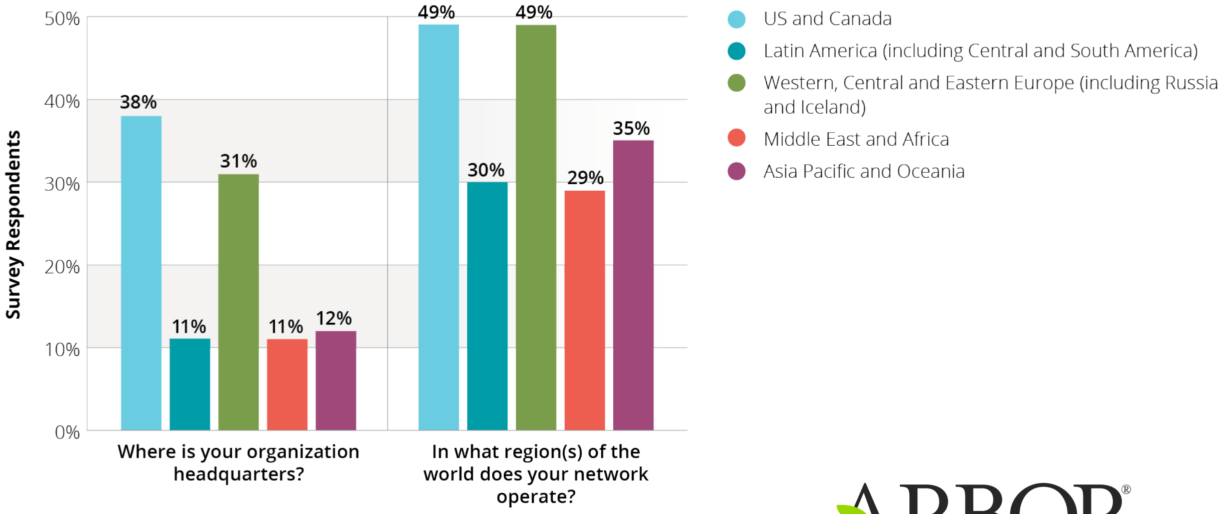


Source: Arbor Networks, Inc.

- 354 global network operators
  - up from 287 last year
- 2/3 Network and Security Professionals

- Nearly half represent EGE
- United States and Canada lead regional participation, Europe a close second
- APAC, LATAM, Middle East and Africa about one-third

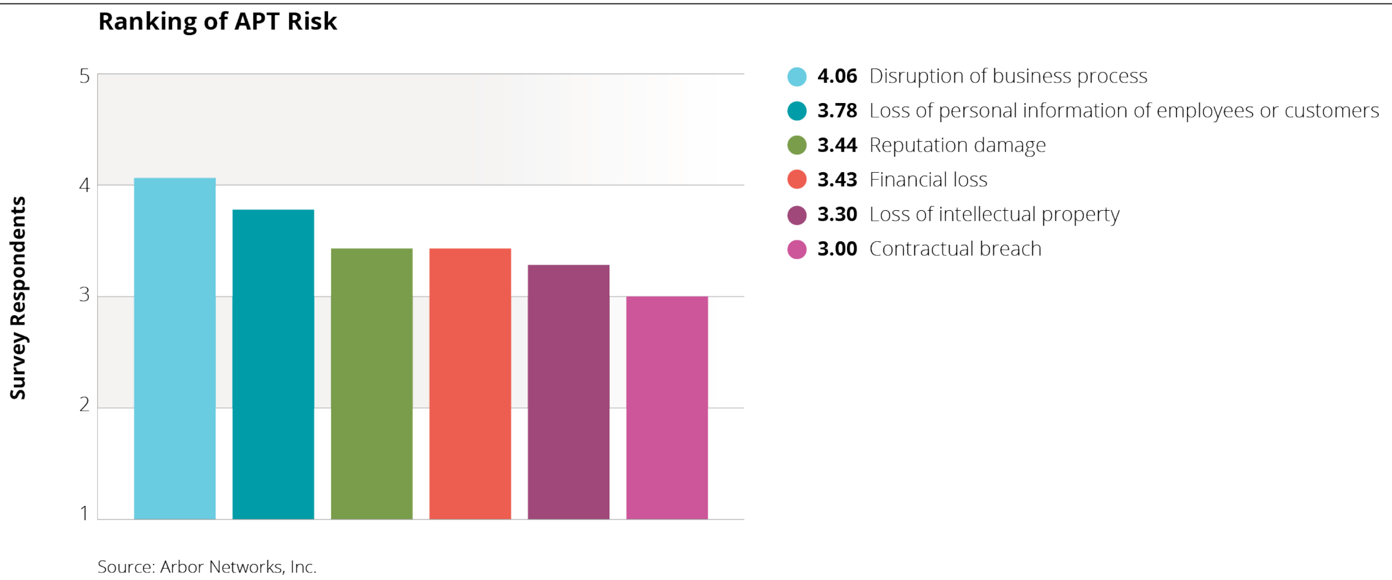
Organization's Geographic Information



Source: Arbor Networks, Inc.

ARBOR® NETWORKS

ADVANCED THREATS

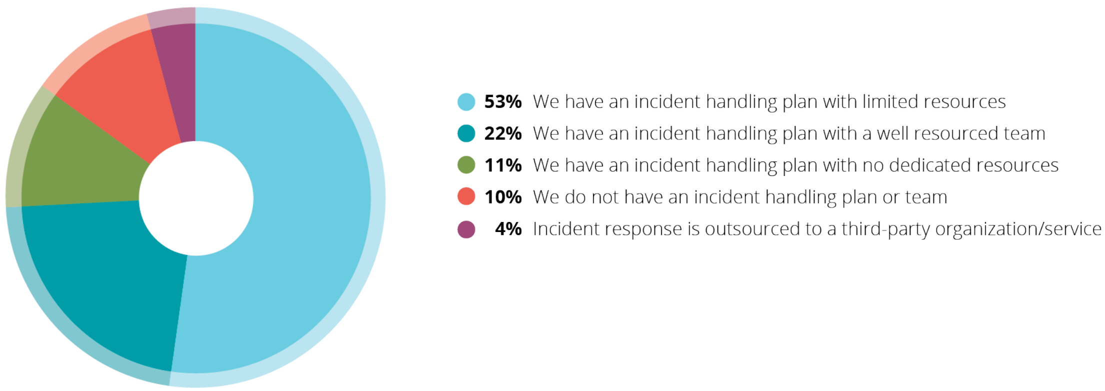


Source: Arbor Networks, Inc.

- The proportion of enterprises seeing APT grew from 18% to 23%
  - Respondents seeing malicious insiders also increase to 17% this year, vs. 12% last
- Advanced threats are one of the top concerns for enterprise organizations overall, however:
  - Banking respondents put disclosure of regulated data top
  - Government put accidental data loss top
- 85% of respondents now have formal breach notification processes in place
- Loss of personal information and/or disruption of business processes are perceived as the top business risks from an advanced threat

INCIDENT RESPONSE

Incident Response Posture

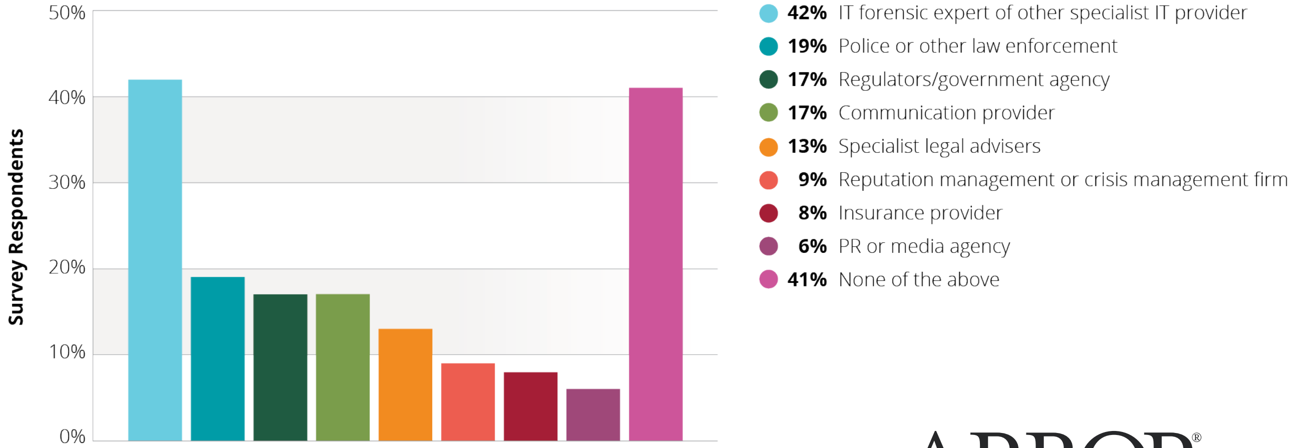


Source: Arbor Networks, Inc.

- Incident response planning up from 68% to 75% this year
- 28% of EGE* see increased incident rate
- EGE respondents with NO preparations for incidents falls from 10% to 6%

- Nearly half contract external assistance w/incident response
- IT forensics most common

Incident Response Assistance

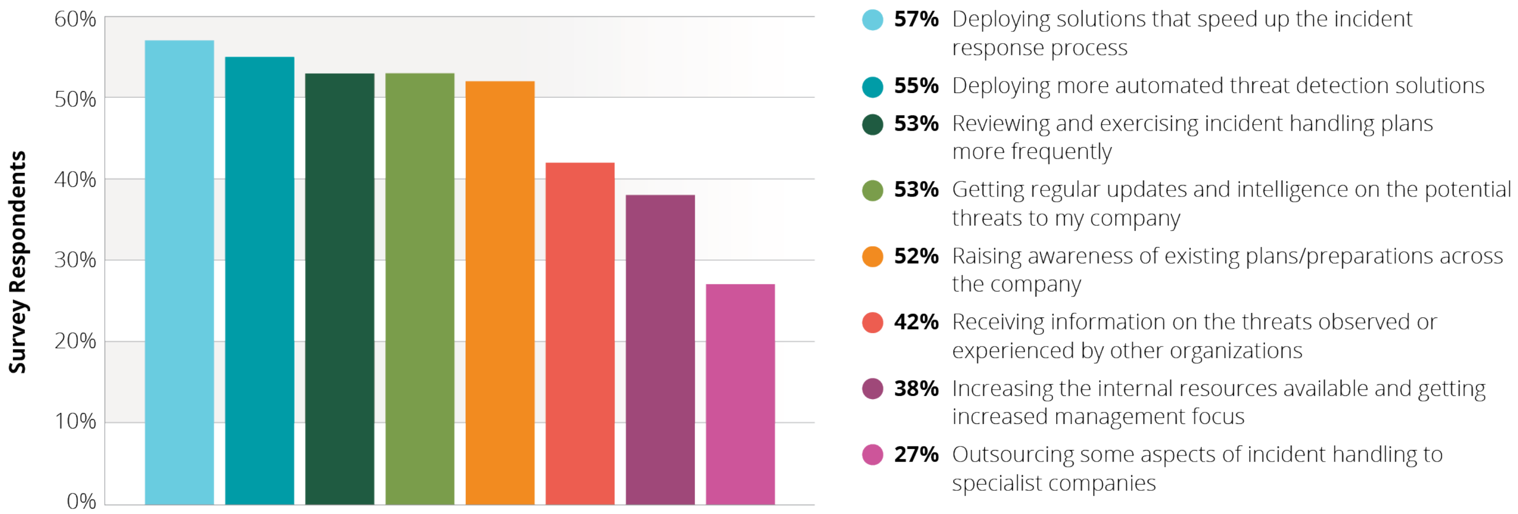


Source: Arbor Networks, Inc.

*EGE: Enterprise, Government, Education respondents

INCIDENT RESPONSE IMPROVEMENT

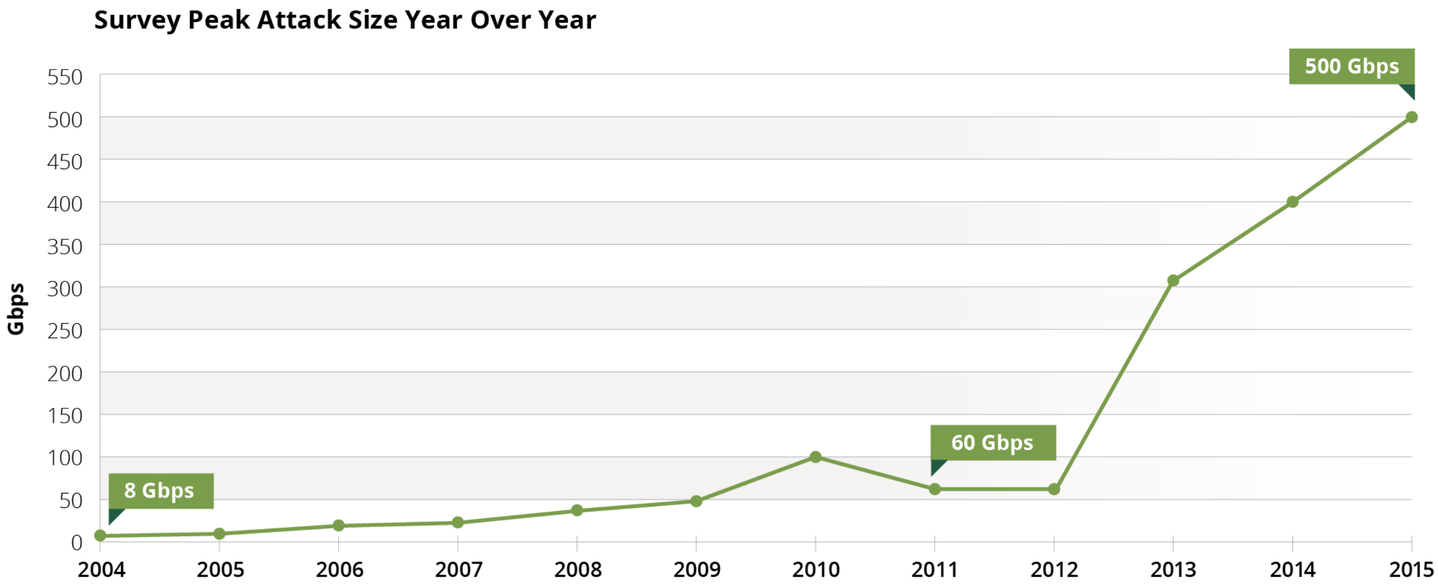
Improving Preparedness



Source: Arbor Networks, Inc.

- This year 57% (up from 45%) of respondents are looking for solutions to speed up the incident response process
  - Last year, deploying additional automated threat detection solutions was the top way respondents were looking to improve incident response times
- Significant drop in respondents looking to increase internal resources to improve incident preparedness, down from 46% to 38%

DDOS - GROWTH CONTINUES

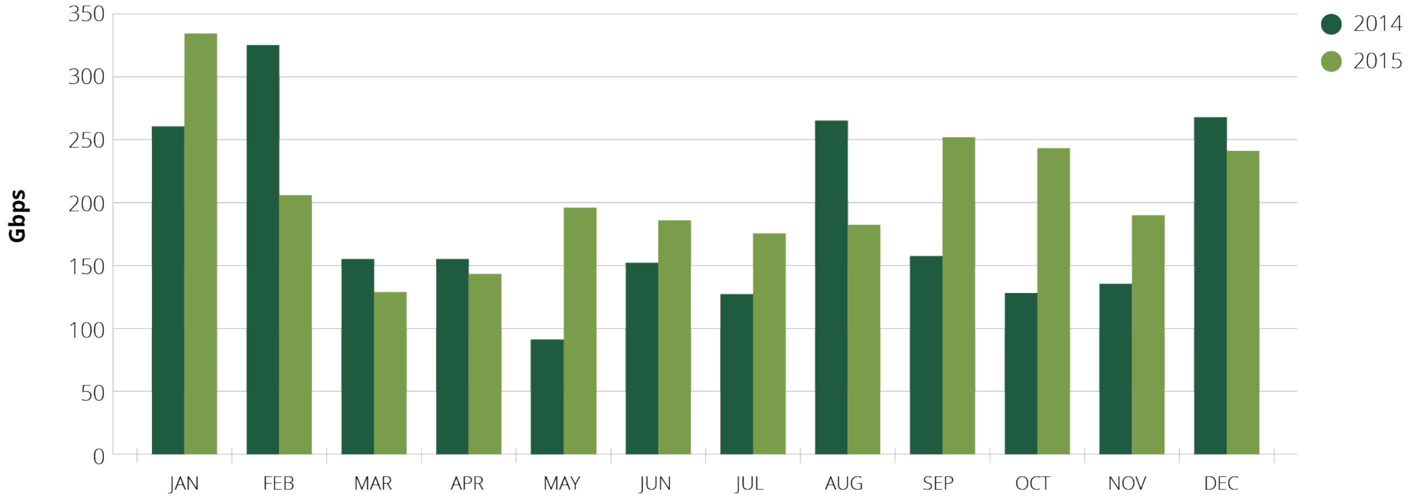


Source: Arbor Networks, Inc.

- 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 report peak attacks over 100Gbps
- Over half of EGE and data center respondents (respectively) saw attacks that completely saturated their Internet connectivity

DDOS GROWTH, ATLAS PERSPECTIVE

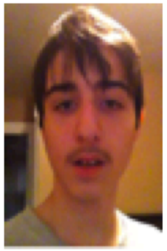
Peak Attack Sizes 2014/2015



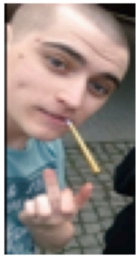
Source: Arbor Networks, Inc.

- 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

DIAMOND MODEL OF DDOS (IOT) BRAZIL



@iceman4391



@bc2fast

@iceman4391 (aka Brandon) <-> ¿@bc2fast?

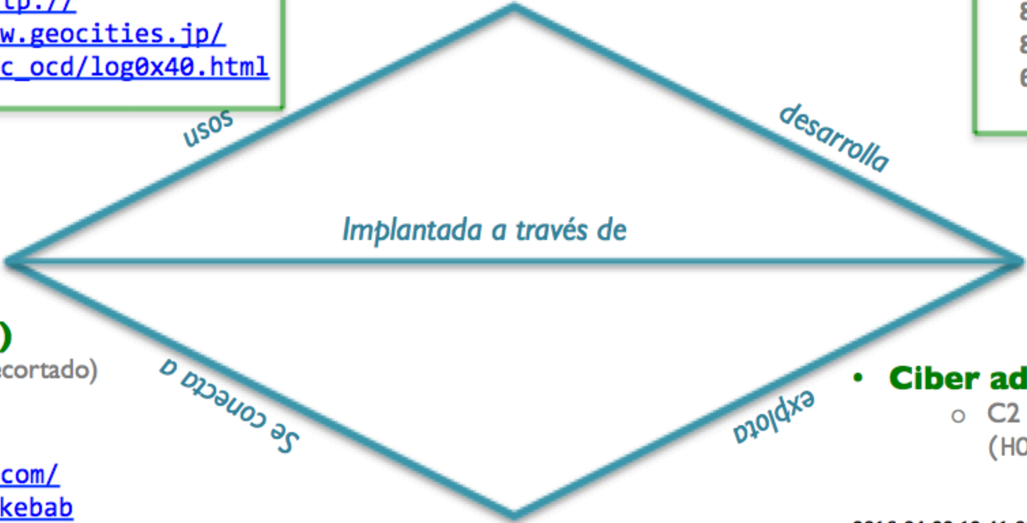
- http://ddos.yt
- http://www.geocities.jp/arc_ocd/log0x40.html

- **Distribuido geográficamente**

Adversario

Más de 1351 fuentes únicas

774	Vietnam
128	Brasil
81	Turquía
80	Rumanía
67	Taiwan



Infraestructura

- **Infraestructura Bots (IoT)**
  - Admin de Cámaras (Linux Recortado)
- **Botnet IRC**
  - Variante de Lizard Stresser
    - https://github.com/gh0std4ncer/lizkebab
  - 2 Servidores de botmasters usando comandos por IRC
    - Holanda Quasi Networks

Capacidades (TTP)

- **Ciber adversario mediano**
  - C2 Comandos de ataque de DDoS (HOLD/JUNK/UDP/TCP)
    - UDP 443 → bankline.itau.com.br: 443: 1400 bytes (chr) RND

```
2016-04-22 12:41:33.276686: !* HOLD 200.*.*.* 443 120
2016-04-22 12:49:27.487482: !* UDP 200.*.*.* 80 120 32 1400 10
2016-04-22 13:11:28.938349: !* TCP 200.*.*.* 443 120 32 syn 1 10
```

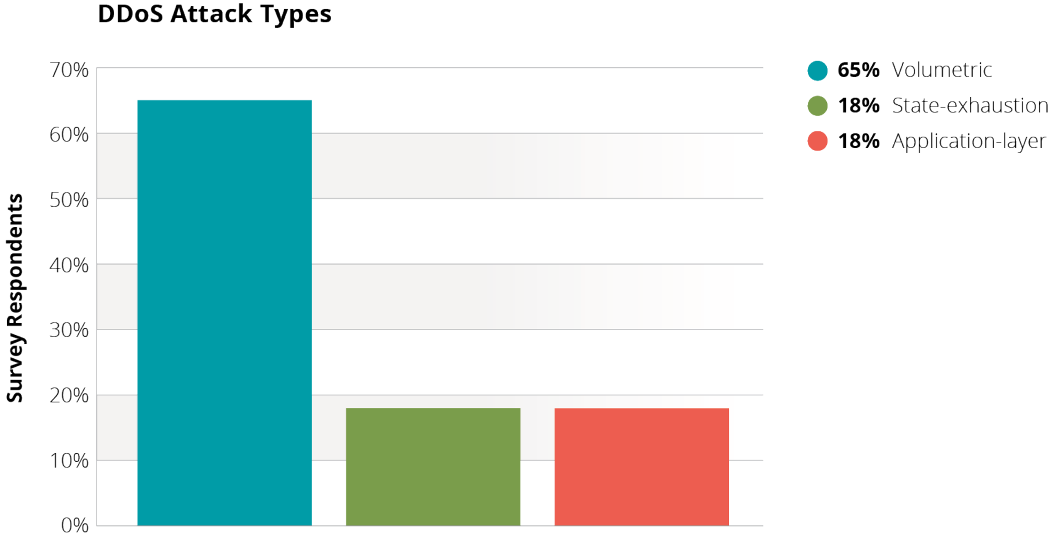
  - Escaner para encontrar otros dispositivos IoT vulnerables con root como contraseña de superusuario
  - Mecanismos para ejecutar comandos de shell

Víctima

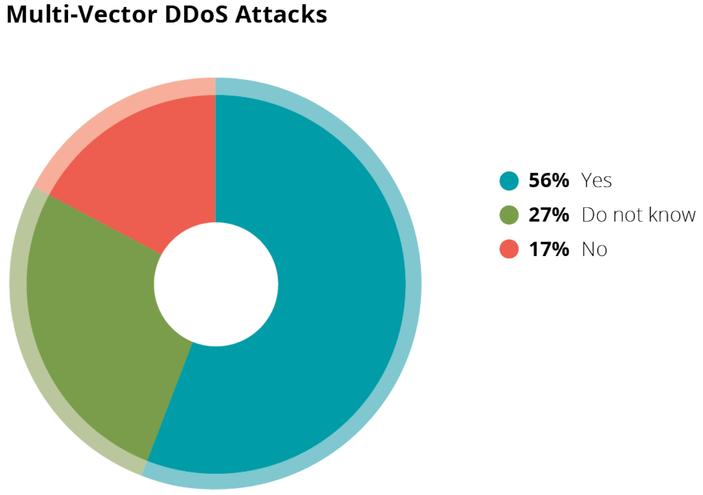
Instituciones financieras, gubernamentales e ISP's en Brasil principalmente

> 300 Gbps ¡No amplificados!

DDOS – COMPLEXITY INCREASES



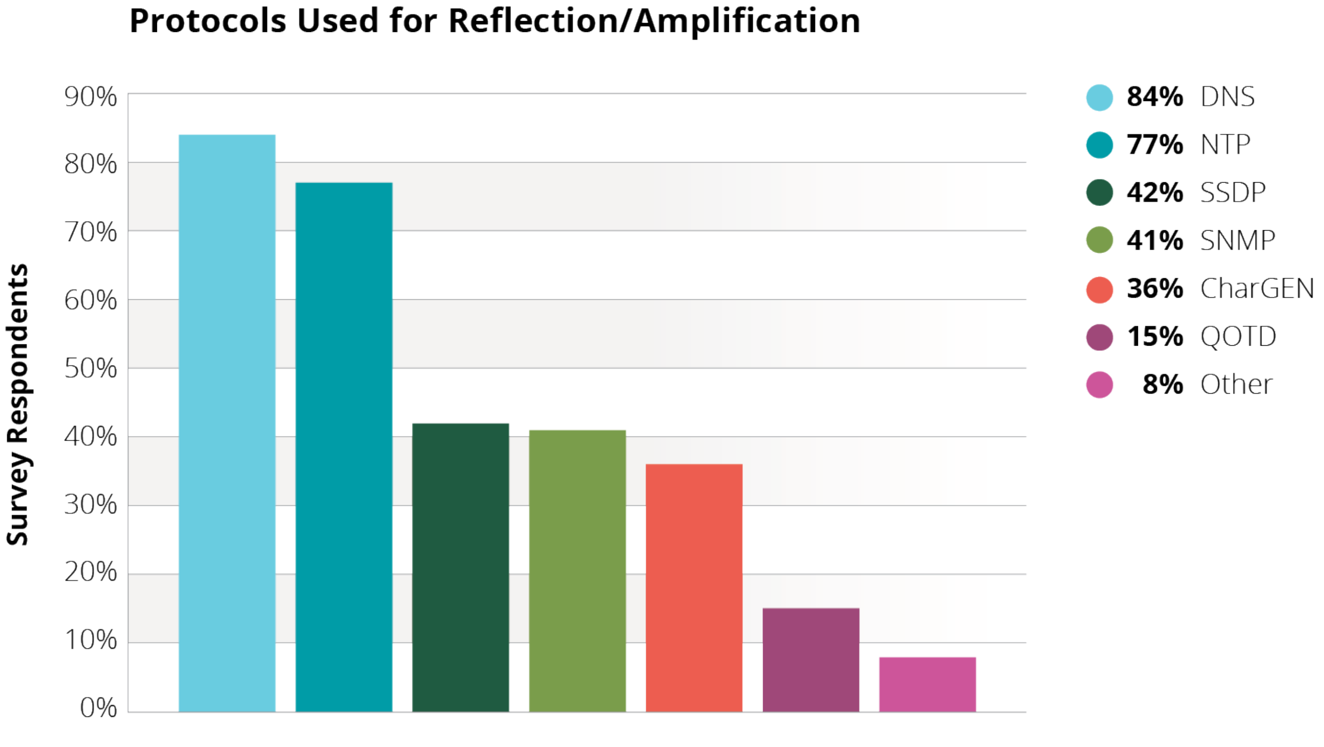
Source: Arbor Networks, Inc.



Source: Arbor Networks, Inc.

- Media focus on volumetric attacks, stealthy application-layer attacks haven’t gone away
  - 93% of respondents see application-layer attacks, up from 90% last year and 86% 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%
- 56% see multi-vector attacks, up from 42% last year

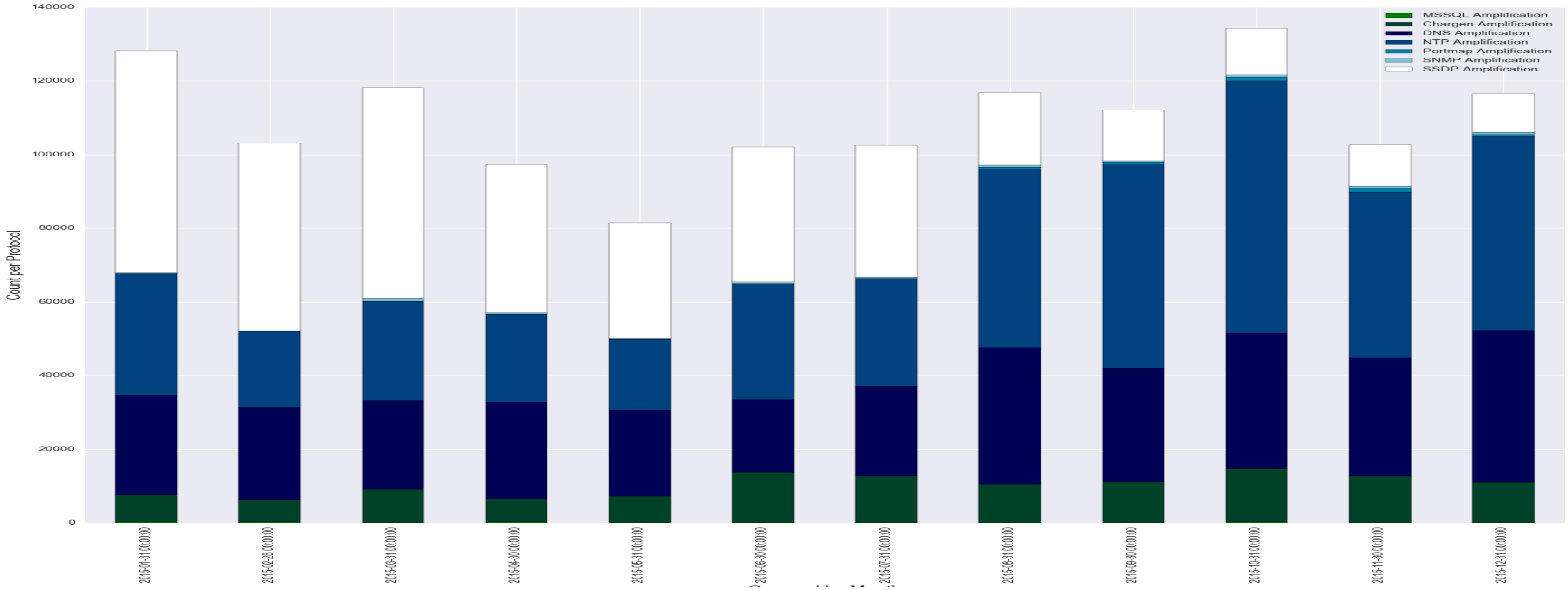
DDOS – REFLECTION AMPLIFICATION



Source: Arbor Networks, Inc.

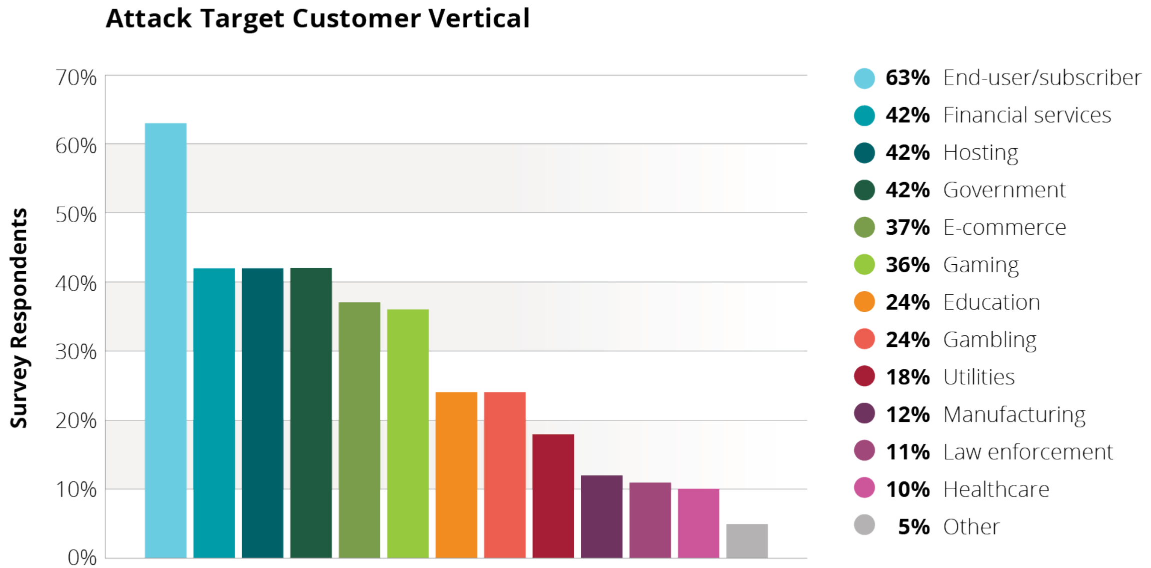
- Reflection amplification attacks are still a key issue.
- Respondents see DNS as most common protocol, closely followed by NTP
- Significant use of SSDP, SNMP and Chargen also reported

REFLECTION AMPLIFICATION, ATLAS VIEW



- NTP, SSDP and DNS are most commonly used protocols
- More than 50K SSDP attacks tracked per month in Q1
- 252Gbps SSDP attack, largest tracked reflection amplification
- More than 55K NTP attacks in Sept / Oct '15
- Average attack at just under 2Gbps

DDOS - TARGETS

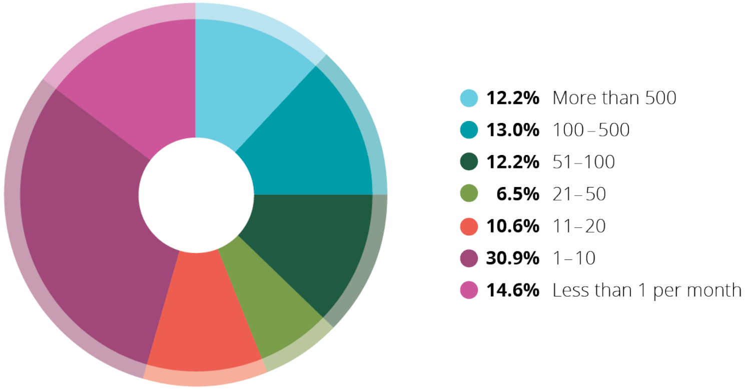


Source: Arbor Networks, Inc.

- 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 attacks against IPv6 services 9% reporting vs. 2% last year

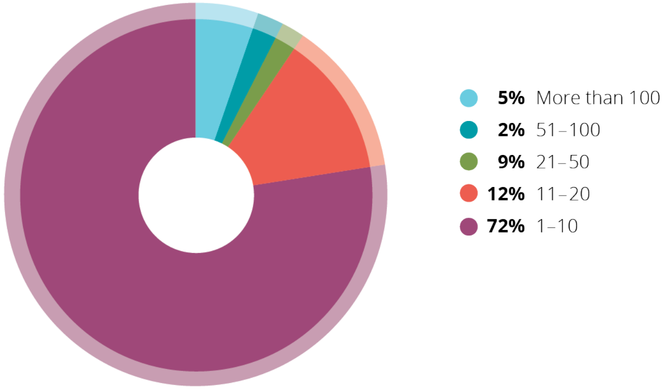
DDOS - ATTACK FREQUENCY

SP DDoS Attack Frequency



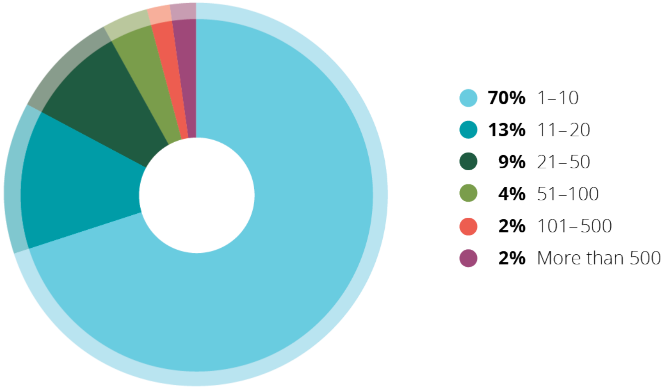
Source: Arbor Networks, Inc.

EGE DDoS Attack Frequency



Source: Arbor Networks, Inc.

Data Center DDoS Attack Frequency

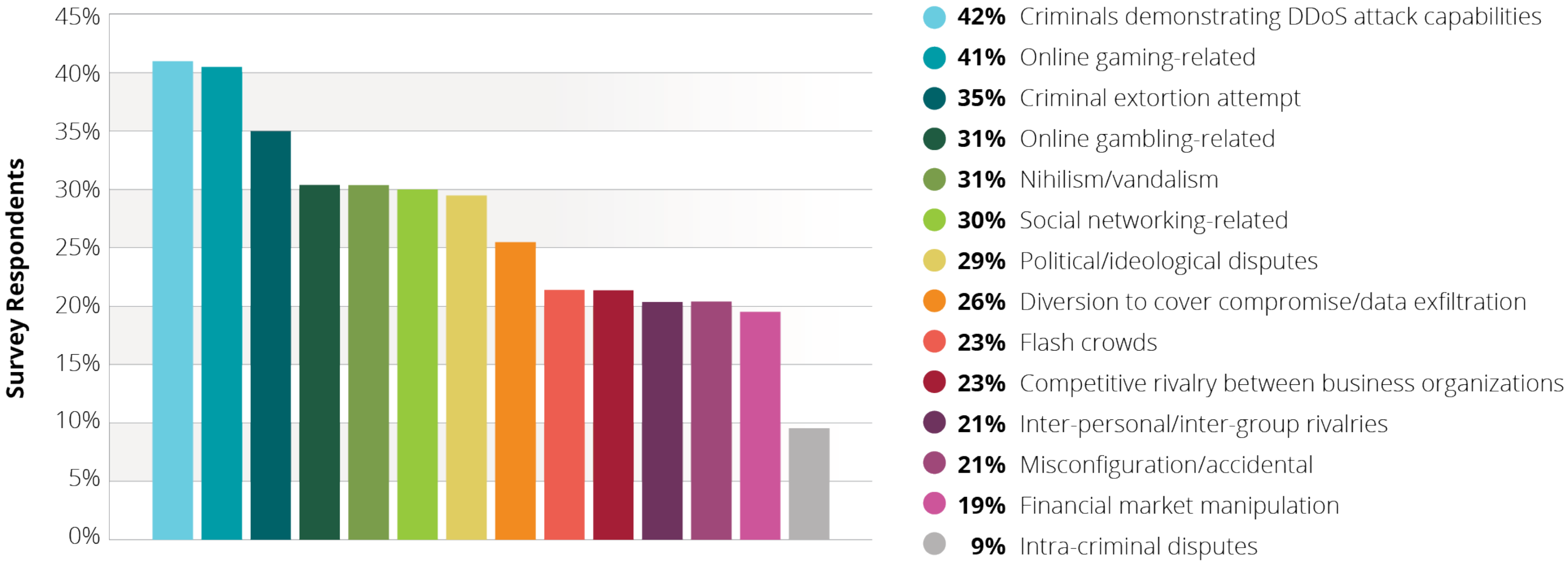


Source: Arbor Networks, Inc.

- 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

DDOS - MOTIVATIONS

SP DDoS Attack Motivations

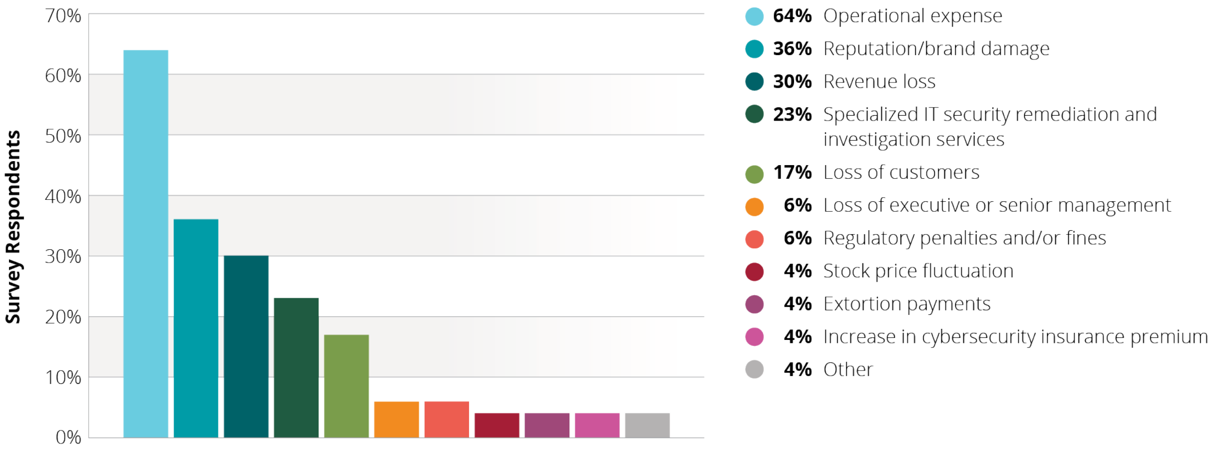


Source: Arbor Networks, Inc.

- 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 - BUSINESS IMPACT

Business Impacts of DDoS Attacks

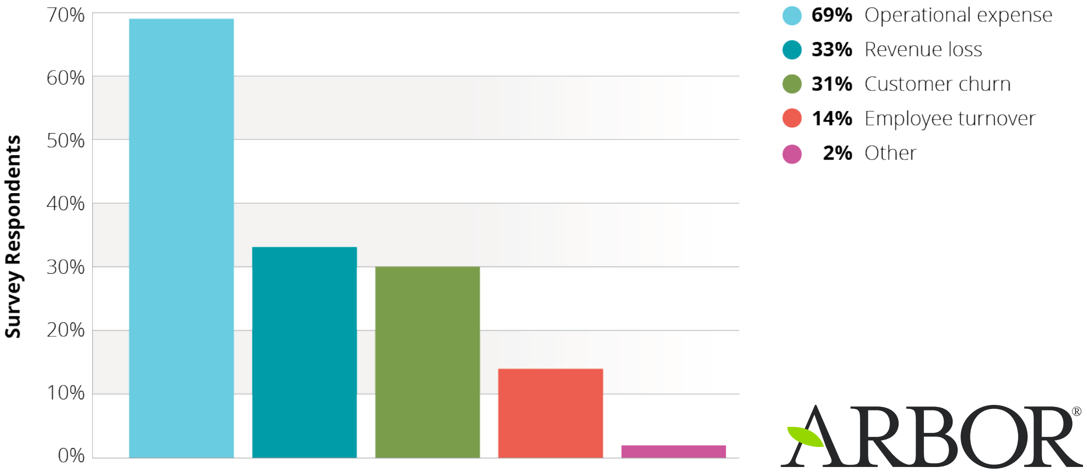


Source: Arbor Networks, Inc.

- 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
- 34% of data centers see outbound attacks, up from 24% last year

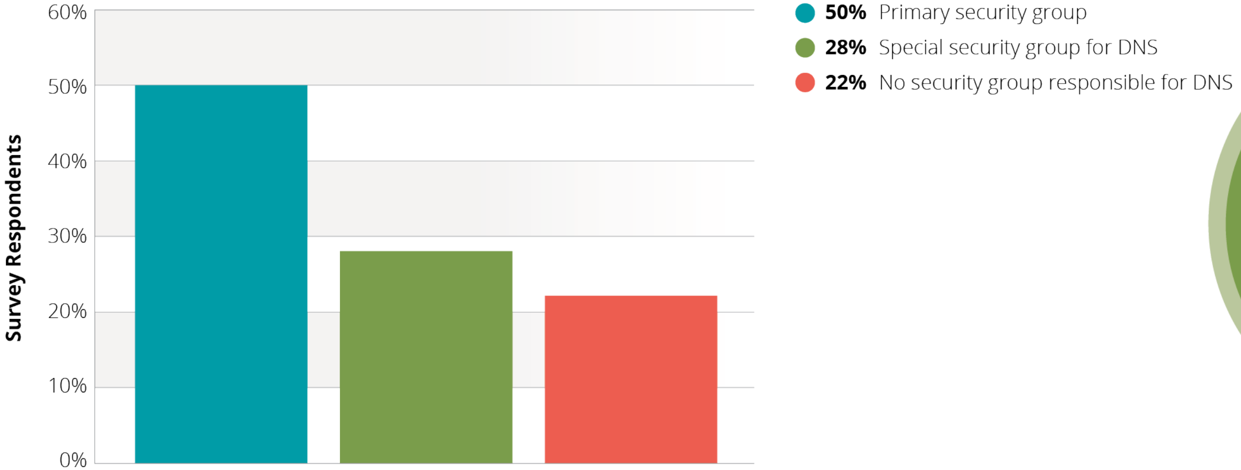
Data Center DDoS Business Impact



Source: Arbor Networks, Inc.

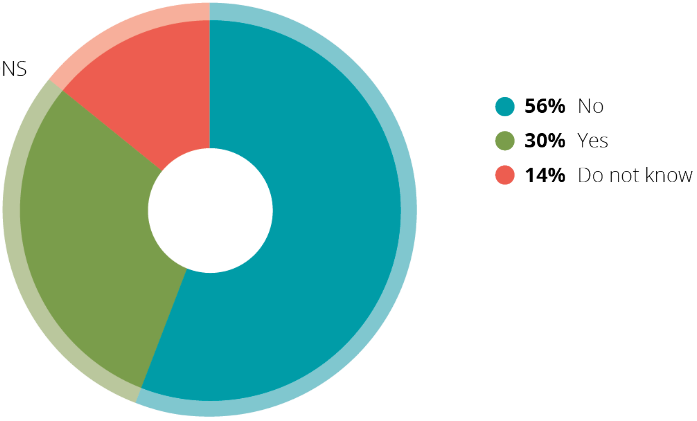
DNS SERVICES

DNS Security Responsibility



Source: Arbor Networks, Inc.

DNS Infrastructure DDoS Attack

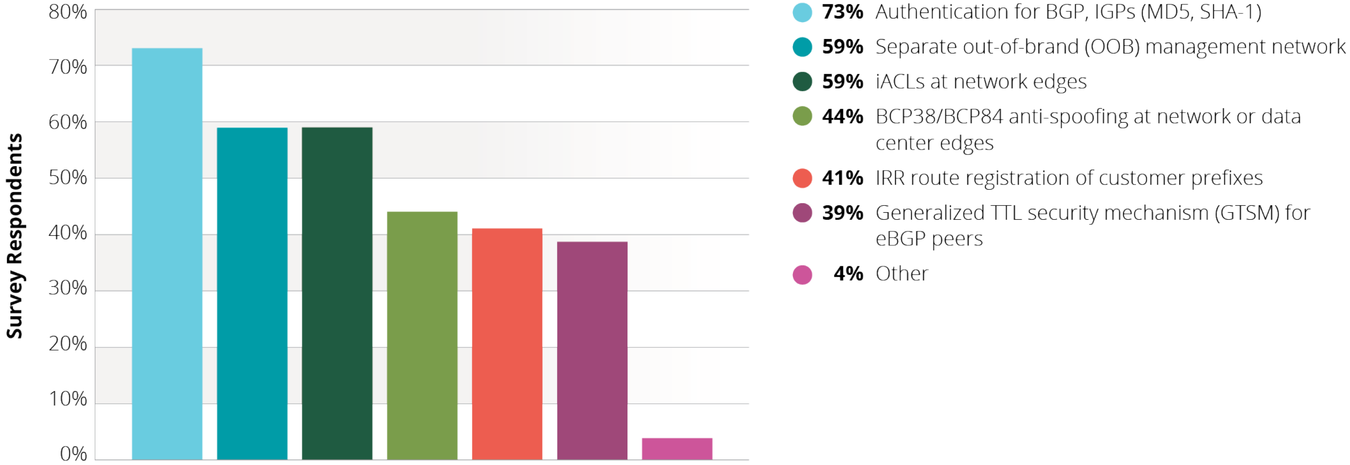


Source: Arbor Networks, Inc.

- DDoS attacks against DNS infrastructure that resulted in a customer visible outage, up from 17% last year to 30% this year
  - This increases further to around a half of respondents if we look purely at service providers.
- Increased resources for DNS security
  - However, 17% of service providers and 26% of enterprises still have no dedicated resources

ORGANIZATIONAL SECURITY

Security Best-Practices



Source: Arbor Networks, Inc.

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

SURVEY HIGHLIGHTS

- Incident Response times are improving, as are investments in technology to speed up the process
- Advanced threats are top concern for enterprise organizations
  - Loss of personal information and/or disruption of business processes perceived as top business risks from advanced threat.
- Largest reported DDoS attack jumps to 500Gbps
  - Over 60X increase from 8Gbps eleven years ago!
- Application-layer attacks monitored by nearly all service providers
  - 56% saw multi-vector attacks, up from 42% last year
- Existing infrastructure, such as firewall and IPS devices, continue to be targeted by DDoS attacks
  - Over half of enterprises and data centers report these devices failing as a result of a DDoS attack - up significantly from 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% last year

ARBOR®

NETWORKS

The Security Division of NETSCOUT