Arbor Networks 12th Annual

WORLDWIDE INFRASTRUCTURE SECURITY REPORT

SURVEY HIGHLIGHTS

This document provides a summary of the results of Arbor Networks' 12th annual *Worldwide Infrastructure Security Report* (WISR). The WISR offers direct insights 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 they face daily and the strategies adopted to address and mitigate them.

INNOVATION AND EXPLOITATION FUEL THE DDoS ATTACK LANDSCAPE

The innovation in the DDoS threat landscape persists as attacks continue to grow in size, frequency and complexity. The inherent security weakness in IoT devices and the release of the Mirai botnet source code both fueled attacker innovation and changed the stakes for businesses focusing much needed attention on DDoS defense and best practices.

Scale

The largest attack reported was 800 Gbps, a 60 percent increase over last year. Since Arbor began the *Worldwide Infrastructure Security Report* in 2005, DDoS attack size has grown 7,900 percent, for a CAGR of 44 percent. In the past five years, DDoS attack size has grown 1,233 percent, for a CAGR of 68 percent.

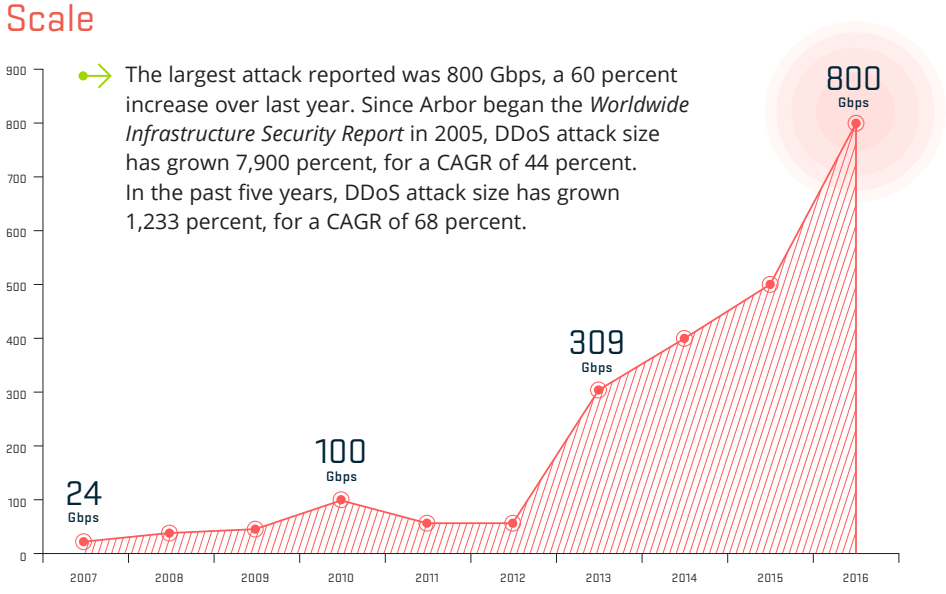

Figure 1 *Peak Attack Size (Gbps)*

ARBOR NETWORKS
The Security Division of NETSCOUT

Frequency

Unfortunately, the chances of being hit by a DDoS attack have never been higher, with respondents showing increased rates of attack.

SERVICE PROVIDERS

53%

Indicated they are seeing **more than 21 attacks per month** — up from 44 percent last year.

ENTERPRISE, GOVERNMENT + EDUCATION (EGE)

45%

Experience **more than 10 attacks per month** — a 17 percent increase year over year.

DATA CENTER

21%

See **more than 50 attacks per month** versus only 8 percent last year.

The massive growth in attack size has been driven by the emergence and weaponization of IoT botnets as well as increased attack activity on all reflection amplification protocols. Reflection amplification can be used by an attacker to multiply attack traffic by hundreds of times, while hiding the original source. For example, an attacker sends 1 Gbps of initial traffic, 100 Gbps is delivered to the target.

- DNS remains the most commonly used reflection protocol, with NTP close behind.
- The results also show heavy use of SSDP, Chargen and SNMP — with the use of Chargen growing most rapidly year over year.

Complexity

Most people think of DDoS attacks as simply flooding network capacity. Today, thanks to attacker innovation, new tools and the ready availability of "booter/stresser" attack services, DDoS attacks are far more complex.

Multiple simultaneous attack vectors are used to target different aspects of victim's infrastructures. These multi-vector attacks are popular because they can be difficult to defend against and are often highly effective, driving home the need for an agile, multi-layer defense.

- Sixty-seven percent of Service Providers reported seeing multi-vector attacks on their networks — a significant rise from 56 percent last year and 42 percent the year before.
- Forty percent of Enterprise, Government and Education respondents witnessed multi-vector attacks.
- Application-layer attacks were monitored by nearly all (95 percent) Service Provider respondents. The most common services targeted by application-layer attacks are DNS, HTTP and secure web services (HTTPS).

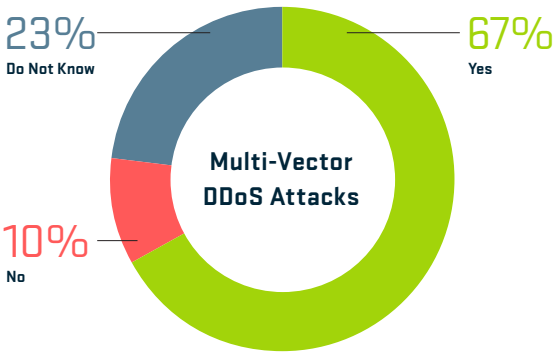

Figure 2 *Multi-Vector DDoS Attacks*

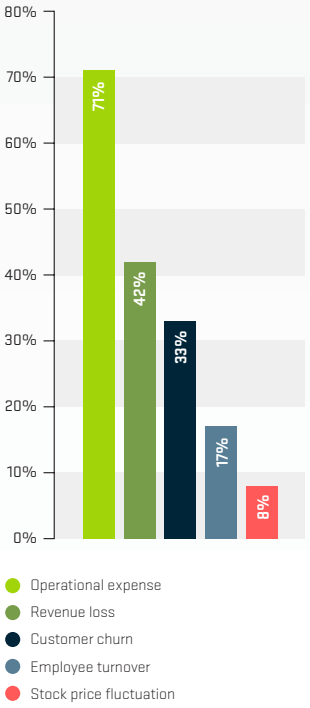

Figure 3 *Data Center DDoS Business Impact*

CONSEQUENCES OF DDoS ATTACKS ARE RISING

In 2016, we saw a DDoS attack, launched from the Mirai IoT botnet, target DNS infrastructure and render many of the internet's leading web properties effectively unreachable. This was front-page news and not just another technology story bringing DDoS defense to the attention of the C-suite and Board of Directors.

- Seventy-eight percent of Service Providers reported more demand from enterprise customers for DDoS managed services.
- Sixty-one percent of Data Center/Cloud Providers reported attacks that fully saturated data center bandwidth, illustrating the importance of a good DDoS protection strategy.
- Costs of a major DDoS attack were cited by nearly 25 percent of Data Center/Cloud providers as exceeding $100,000, while 5 percent noted costs in excess of $1 million.
- Forty-one percent of EGE respondents reported DDoS attacks exceeding their total internet capacity. Nearly 60 percent estimate downtime costs above $500/minute, with some indicating much greater expense.

MORE APPRECIATION OF RISK = BETTER BEHAVIOR

Survey results indicate a better understanding of the brand damage and operational expense incurred due to successful DDoS attacks, driving focus on best-practice defensive strategies.

In recent years, many infrastructure security solutions have bolted-on DDoS protection capabilities. While IPS devices and firewalls effectively address network integrity and confidentiality, they fail to address a fundamental concern regarding DDoS attacks — network availability. Across the board, there was a marked decrease in the use of firewalls, IPS devices and load balancers for DDoS protection.

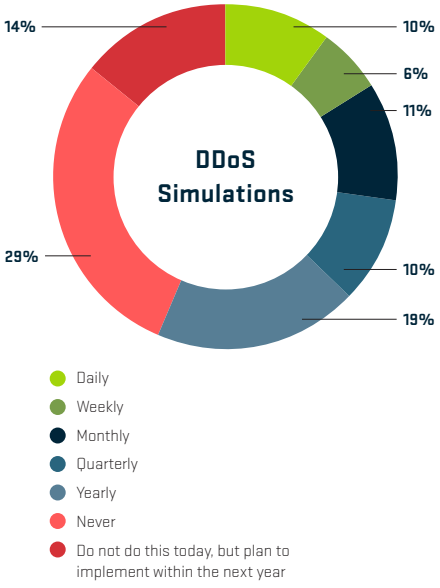

Figure 4 *DDoS Simulations*

Service Provider

- Eighty-three percent are utilizing intelligent DDoS mitigation solutions (IDMS).
- Seventy-six percent use IDMS to mitigate IPv6 attacks.
- Fifty-seven percent carry out DDoS defense simulations, up from 46 percent last year and one of the highest levels in the last four surveys.
- The practice is paying off. The proportion of respondents able to mitigate attacks in less than 20 minutes has increased to 77 percent, up from 74 percent last year and 68 percent the year before.

SURVEY SCOPE + DEMOGRAPHICS

01/ WISR Survey Data

Based upon 356 responses from a mix of tier 1 and tier 2/3 service providers, as well as hosting, mobile, enterprise and other types of network operators from around the world.

02/ Survey Respondents

As in previous years, two-thirds of all respondents identify as security, network or operations professionals.

03/ Timeframe

Data covers November 2015 through October 2016.

Enterprise, Government + Education

- Firewalls, load balancers and CDNs all tied for last place in effectiveness at mitigating DDoS attacks.
- Nearly half had firewalls or IPS devices experience a failure or contribute to an outage during an attack, similar to last year.
- Nearly 55 percent now carry out DDoS defense simulations, with around 30 percent conducting them at least quarterly.
- Forty-four percent are deploying IDMS solutions, 30 percent deploy best-practice hybrid defense and 26 percent utilize an "always-on" device or service.

Data Center/Cloud Providers

- The proportion using firewalls for DDoS defense has fallen from 71 percent to 40 percent.
- Forty-three percent saw firewalls or IPS/IDS devices experience or contribute to an outage during a DDoS attack.

ARBOR NETWORKS
The Security Division of NETSCOUT

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales
Toll Free +1 855 773 9200

Europe
T +44 207 127 8147

Asia Pacific
T +65 68096226

www.arbornetworks.com

SR/WISR2016SUMMARY/en/0117-Letter

ABOUT ARBOR NETWORKS

Arbor Networks, the security division of **NETSCOUT**, is driven to protect the infrastructure and ecosystem of the internet. It is the principle upon which we were founded in 2000; and remains the common thread that runs through all that we do today. Arbor's approach is rooted in the study of network traffic. Arbor's suite of visibility, DDoS protection and advanced threat solutions provide customers with a micro view of their network enhanced by a macro view of global internet traffic and emerging threats through our ATLAS infrastructure. Sourced from more than 300 service provider customers, ATLAS delivers intelligence based on insight into approximately 1/3 of global internet traffic. Supported by Arbor's Security Engineering & Response Team (ASERT), smart workflows and rich user context, Arbor's network insights help customers see, understand and solve the most complex and consequential security challenges facing their organizations.