



## DDoS Attacks Exceed 100 Gbps, Attack Surface Continues to Expand

By [Mike Lennon](#) on Feb 01, 2011

2010 should be viewed as the year distributed denial of service (DDoS) attacks became mainstream, says **Arbor Networks**. In its *Sixth Annual Worldwide Infrastructure Security Report*, released today, Arbor Networks revealed that DDoS attack Size broke **100 Gbps** for first time; **up 1000% Since 2005**.

The year witnessed a sharp escalation in the scale and frequency of DDoS attack activity on the Internet with many high profile attacks launched against popular Internet services and other well known targets. In addition to hitting the 100 Gbps attack barrier for the first time, application layer attacks hit an all-time high.

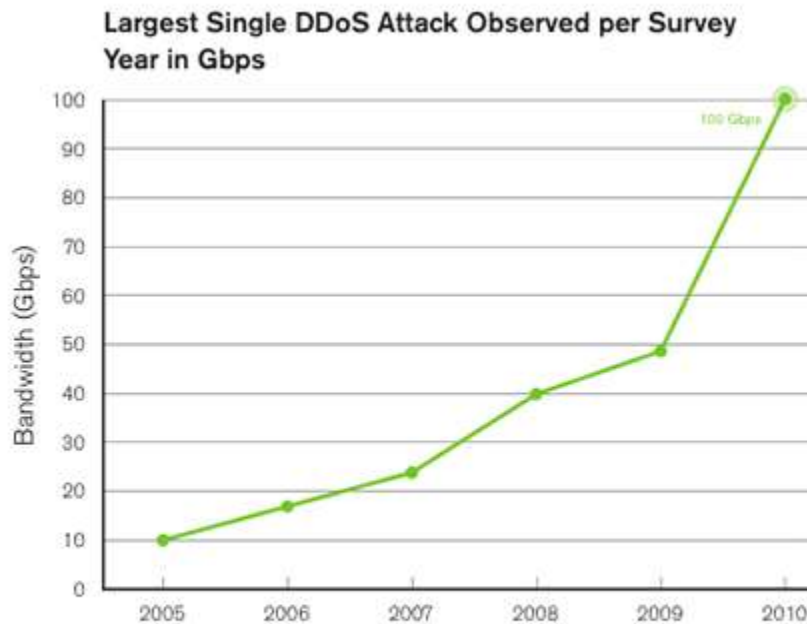


Figure 1  
Source: Arbor Networks, Inc.

“Nowadays, it is frighteningly easy for attackers to execute a DDoS attack. Botnets comprised of thousands of compromised PCs can be rented cheaply, and software capable of automating attacks can be acquired readily on the underground market,” [writes Ram Mohan](#), EVP and CTO

DDoS Attacks are the risks that F5’s ASM (Application Security Manager) mitigates in a double-security fashion. To discuss further, call Milestone Systems, Inc. 877-771-9510



**milestone**  
systems, inc.

at Afilias and a regular *SecurityWeek* contributor. "A distributed denial of service attack is every business's worst nightmare. One minute, everything is ticking along as normal. The next, your infrastructure is hit by a tsunami of spurious traffic from across the Internet. Legitimate users find themselves locked out, your ability to do business online grinds to a halt, and there's not a great deal you can do about it – unless you prepare ahead of time."

Arbor Networks suggests that Botnet-driven DDoS attacks are likely to continue as a low cost, high-profile form of cyber-protest in 2011 and beyond. Major incidents in 2010 included DDoS attacks associated with the territorial disputes between China and Japan, the ongoing political turmoil in Burma and Sri Lanka and the WikiLeaks affair. The need to protect availability has finally made it onto the radar screen of enterprise IT consulting firms worldwide, and DDoS defense has consequently reached the status of a CXO-level issue globally.

### **Other Highlights from the Arbor Networks Sixth Annual Worldwide Infrastructure Security Report:**

**Attack surface continues to expand** - The DDoS attack surface describes all aspects of network infrastructure, servers, protocols and services that are vulnerable to DDoS attacks. As new equipment, protocols and services are introduced into networks, the vulnerable attack surface for DDoS is expanded. This presents a significant challenge for network operators. Botnet-driven volumetric and application-layer DDoS attacks continue to be the most significant problems facing operators. This year's report also reveals attackers are targeting the infrastructure itself, specifically DNS, VoIP and IPv6. "Network operators are facing a global Internet insurgency driven by the ubiquity of botnets. This has led to rapidly escalating DDoS attack size, frequency and sophistication," said Roland Dobbins, solutions architect with Arbor Networks. "Adding to the challenges facing operators is the increasing number of attack vectors, including applications and services, not to mention the proliferation of mobile devices."

**Application-layer DDoS attacks are increasing in sophistication and operational impact** - An alarming 77% of respondents detected application layer attacks in 2010. These attacks are targeting both their customers and their own ancillary supporting services, such as domain name system (DNS), Web portals, etc. Internet data center (IDC) operators and mobile/fixed wireless operators report that application-layer DDoS attacks are leading to significant outages, increased operational expenditures (OPEX), customer churn and revenue loss.

**Increasingly sophisticated attacks expose IPS and firewall shortcomings** - In an effort to achieve DDoS protection, many operators have deployed stateful firewalls and intrusion prevention system (IPS) devices to protect data center infrastructure. In actuality, these devices can render networks more susceptible to attacks as the state tables on even the most scalable versions available can be overwhelmed with a moderate size DDoS attack. Nearly 49 percent of IDC respondents reported a firewall or IPS outage due to DDoS.

**Lack of preparedness on mobile networks presents new attack opportunities** - The fastest-growing category of Internet service providers (ISP) -- mobile and fixed wireless operators -- may be the least prepared in terms of network visibility and control and overall ability to defend themselves and their customers against attack. Nearly 60 percent of respondents indicated they

have limited or no visibility into the network traffic of their wireless packet cores. In addition, only 23 percent indicated they have visibility into their wireless packet cores on par with, or better than, their visibility into their wireline networks. With some notable exceptions, many mobile/fixed wireless network operators appear to have security postures approximating those of wireline operators eight to 10 years ago.

*Technical Reading: [Designing Security for Newly Networked Devices](#)*

*Related: [Mobile & Smart Device Security Survey](#) - Concern Grows as Vulnerable Devices Proliferate*

### **Operators are struggling to keep up their security posture through [transition to IPv6](#) -**

Operators expressed concern over lack of visibility into IPv6 network traffic and their inability to control that traffic to the same degree they control IPv4 traffic. The additional network state and DDoS vector introduced by deployment of 6-to-4 gateways and network address translators (NATs) is also a significant threat to availability.

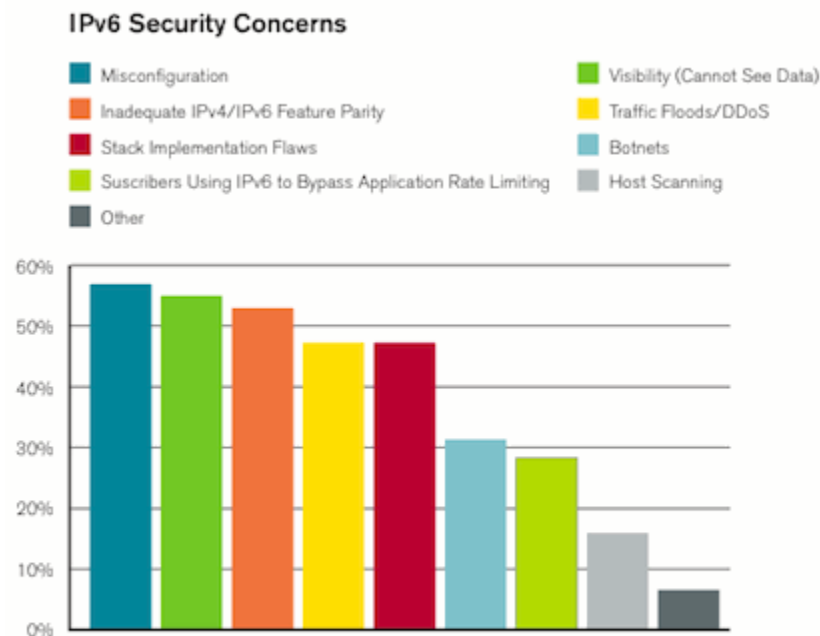


Figure 58  
Source: Arbor Networks, Inc.

**DNS emerging as a top target** - DNS has emerged as one of the easiest ways to DDoS a server/service/application and take it offline by denying Internet users the ability to resolve server/resource records. Additionally, the large number of misconfigured DNS open recursors, coupled with the lack of anti-spoofing deployments on many networks, allows attackers to launch overwhelming DNS reflection/amplification attacks.

The report offers a view into the challenges of network operators on the front lines of a global battle against botnets and DDoS attacks and is available for download at

<http://www.arbornetworks.com/report> ##