



Nearly 3% of Internet traffic causes Distributed Denial of Service (DDoS) attack!

Are you ready for the battle?

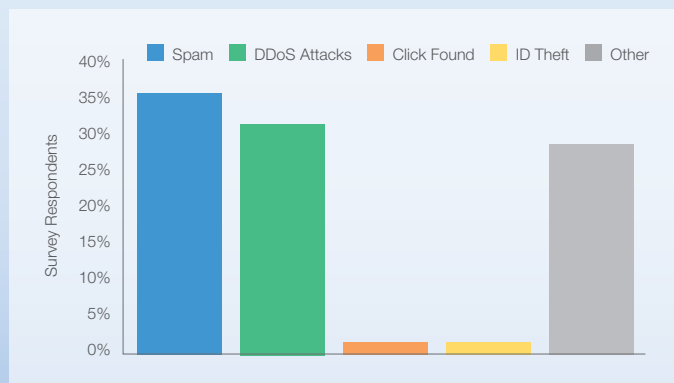
As today's business becomes more and more connected, enterprises want to be online 24 x 7. At the same time, they demand bigger data repository, powerful network to support collaboration tools, and guaranteed delivery of business critical applications.

However, not enough emphasis is being placed on security solutions that protect them against attacks by someone or some external groups, which target at draining their network resources for personal and or criminal gains.

The reality is, a significant portion of Internet traffic today comprises of senseless data which gobble up your bandwidth and "max out" your network resources, and these are certainly not works of benign hackers who are testing the security of your network for leisure.

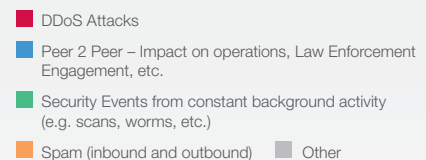
A survey by US-based network security company Arbor Networks said that as much as 10% of email traffic today is spam and about 1–3% is Distributed Denial of Service (DDoS) traffic from zombie hosts computers controlled by hackers with criminal motives. The survey results also found that next to spam attacks, DDOS attacks have also been the next most observed attacks originating from bots (see below).

Observed Bots – Past 12 Months



Source: Arbor Networks, Inc.

Operational Resources Are Strained



- Service providers are facing increasing cost and revenue pressure in a slowing global economy
- Organizations are turning to Managed Security Services (MSS) – network security management from a service provider
- ISPs are increasingly deploying more complex distributed VoIP, video and IP services
- However, surveyed ISP security engineers also say these new services are often poorly prepared to deal with the new Internet security threats



What is Distributed Denial of Service?

But what exactly is DDoS and why is DDoS mitigation high on every enterprise agenda? A DDoS attack is an attempt by a hacker to make computer resources unavailable, either temporarily or permanently to your intended user.

Typically, a hacker will write a program and send it to thousands of agents or zombie hosts – creating a botnet that will, upon the command of the hacker, simultaneously attack a target system. When this happens, this could bring down an electronic stock trading or gaming platform thereby wreaking a large amount of damage to the firm – both financially, as well as destroying its reputation.

Besides consuming computational resources such as bandwidth, disk space or CPU time, a DDoS attack could also disrupt routing, damage other configuration information or reset TCP session which will all affect application performance and availability. Hackers could also disrupt physical network components or obstruct communication media between intended users, thereby preventing parties from communicating effectively. Depending on the industry, downtime could cause companies millions of dollars (see below).

Potential Revenue Loss Due to Downtime

Industry Sector	Revenue/ Hour	Revenue/ Employee Hour
Energy	\$2,817,846.00	\$569.20
Telecommunications	\$2,066,245.00	\$168.98
Manufacturing	\$1,610,645.00	\$134.20
Financial Institutions	\$1,495,134.00	\$1,079.89
Information Technolog	\$1,344,461.00	\$184.03
Insurance	\$1,202,444.00	\$370.92
Retail	\$1,107,274.00	\$244.37
Pharmaceuticals	\$1,082,252.00	\$167.53
Banking	\$996,802.00	\$130.52
Food/Beverage Processing	\$804,192.00	\$153.10
Consumer Products	\$785,719.00	\$127.98
Chemicals	\$704,101.00	\$194.53
Transportation	\$668,586.00	\$107.78
Utilities	\$643,250.00	\$380.94
Healthcare	\$636,030.00	\$142.58
Metals/Natural Resources	\$580,588.00	\$153.11
Professional Services	\$532,510.00	\$99.59
Electronics	\$477,366.00	\$74.48
Construction and Engineering	\$389,601.00	\$216.18
Media	\$340,432.00	\$119.74
Hospitality	\$330,654.00	\$38.62
Average	\$1,010,536.00	\$205.55

Source: Gartner Group
 1 Assumes 2000 hours per year

While most ISPs and enterprises now have the infrastructure to proactively detect bandwidth flood attacks, many still lack the ability to mitigate these attacks which are increasing in scale and effectiveness from the 1–2 gigabits range, to up to about 40 gigabits – the largest attacks recorded by Arbor Networks.

If ISPs, which have the resources to implement advanced network security but are not confident of their ability to mitigate these attacks, imagine how much more difficult it would be for companies that don't have network security resources and expertise, but yet are dependent on the Internet for their core business?

Thankfully, today, there are two effective ways an organization can protect itself against DDoS attacks – Blackhole filtering and Clean Pipe.

Blackhole filtering simultaneously filters enterprise routers within a network, blocks all traffic going to an IP address being attacked and makes the address “invisible” on the Internet. Blackhole is suitable for enterprises that don't rely on one or two IP addresses to support traffic such as an ISP that supports traffic for hundreds or thousands of IP addresses.

The Clean Pipe method, which essentially filters or cleans all traffic before it reaches end users, is suitable for companies that use a limited number of IP address to transmit traffic including gaming companies, banks and Web portal hosts.

Pacnet has recently added DDoS Mitigation to its IP Transit and Internet Service Portfolio offering both Clean Pipe and Blackhole capabilities as value added services to Pacnet's on-Net and Internet Services customers. Targeting ISPs, large enterprises and SMBs, the Pacnet DDoS Mitigation solution spares the customers from the cost and complexity of managing Intrusion Prevention Solutions (IPS) on their premises.

Backed by our large regional backbone network, Pacnet is further able to offer unparalleled Clean Pipe protection on a global/regional scale. Capable of filtering traffic of up to 100Gbps, Pacnet can effectively protect enterprise from large scale and more complex attacks which smaller ISPs will not be able to prevent.

With DDoS attacks becoming a serious enterprise challenge and no company should take it sitting down. By providing a cost effective DDoS mitigation solution, we hope to be able to contribute in the concerted effort to avert the criminal activities that prevent enterprises from thriving in a connected marketplace.

Attacks are on the Rise!

- Attacks are on the rise and more sophisticated – Smaller, more sophisticated attacks cause more disruption in service and are increasingly difficult to mitigate
- Brute Force Attacks are growing exponentially – A 67% increase in attack scale over the last year; 2.5x the size of the largest attack reported last year and 100-fold increase versus 2001
- Botnets are still a concern – 26% continue to be the vehicle for delivering the largest problems to network operations and security engineers
- Operational resources are strained – A significant increase in the managed DDoS detection and mitigation services
- Emerging threats: VoIP and IPv6 – The scale and frequency of security threats for IPv6 will increase as it becomes more widely deployed while VoIP continues to pose a threat, though ISPs are underprepared to address it

Source: Arbor Networks