Where DDoS is a business opportunity

The number of Distributed Denial of Service (DDoS) attacks is rising worldwide, with the average size of a DDoS attack around 1.2Gbps, according to Arbor Networks' Threat Analysis System.

Anton Jacobsz, Managing Director of Arbor Networks distributor Networks Unlimited, says in an attack such as this, Internet Service Providers tend to 'black hole' or switch off the targeted server as quickly as possible, to avoid slowing down services to other customers sharing the affected pipe. "This stops the slowdown of services to other customers, but it also means the attackers achieved their objective – the service under attack goes down," he says.

With constant uptime critically important for a growing number of businesses, having a service down after an attack could mean significant financial losses. "This paves the way for ISPs to step in and mitigate the risk at service provider level," says Jacobz. "Not only is this more effective, it has the advantages of allowing the ISP to offer better customer service."

In an environment where demand for managed security services is growing, ISPs are well positioned to capitalise on the demand for services, says Arbor. He notes that Frost & Sullivan expects the managed security service provider (MSSP) to grow to around $4 billion by 2016 in North America alone, with the managed security and security monitoring services segment yielding the highest percentage of total revenue in the MSSP market. ISPs can expand their revenue by tapping in to this market, says Arbor Networks.

Because ISPs own the pipes that transmit data across the Internet, they are able to deliver a comprehensive solution that can combat the two primary types of DDoS attacks: high-bandwidth 'volumetric' attacks usually generated by Internet bots or compromised PCs grouped together in large-scale botnets; and 'application-layer' DDoS attack that target specific services ranging from Web commerce and DNS services to email and online banking.

Arbor notes that the best place to stop volumetric DDoS attacks is in the ISP cloud (via network-based DDoS protection) because the saturation happens upstream and can only be remediated in the provider's cloud. The best place to perform application-layer DDoS detection is in the data center itself because the attack can only be detected and quickly stopped at the data-center edge. Only ISPs can provide both a network-based service component to stop volumetric DDoS attacks and a CPE-based service component to stop application-layer DDoS attacks—representing a distinct competitive advantage.

Jacobsz says: "If service providers implement protection solutions across the installed base they are able to offer cost efficiencies and better risk mitigation to their customers. When an ISP is already supplying a managed firewall, Secure Socket Layer virtual private network (SSL VPN), intrusion detection system (IDS), intrusion prevention system (IPS) and other security measures, adding an incremental managed DDoS protection service can be relatively straightforward and cost-efficient."