Filtering criminal dDOS attacks

June 23 2014

A new hybrid filtering system to protect cloud computing services from distributed denial of service (dDOS) attacks has been developed by US and Indian researchers. They provide details in the latest issue of the International Journal of Grid and Utility Computing.

A distributed denial of service (dDOS) attack usually involves a network of computers infected with malware (a botnet) sending repeated data requests en masse to a single server. The botnet is usually controlled by activists intent on protesting against a particular company or organization, by hackers intent on breaching the security of the target system and opening a back door to allow them access to private or proprietary information. According to tech news site Crunchbase, numerous sites have succumbed to dDOS attacks and been thrown offline for various reasons, they include local networking site Meetup, project management tool Basecamp, video site Vimeo, link shortener Bit.ly, blogging system SAY Media/TypePad, internet domain registrar Namecheap, online dating site Plenty of Fish and search engine optimization company Moz, there are many others and many smaller companies are attacked on a daily basis. Many recent dDOS attacks have exploited unpatched security loopholes in networking protocols.

Recently, however, various cloud-based internet services including newsreader website, Feedly, online notebook and bookmarking tool Evernote were taken offline by criminals intent on extorting money from them in exchange for halting the attack. Both companies and others that were attacked this week responded by bravely refusing to give in to the criminals and fought against the dDOS by various means, switching

servers, putting up additional filters and firewalls. The attack is still under way at the time of writing.

Meanwhile, Ajith Abraham, Director of Machine Intelligence Research Labs (MIR Labs) in Auburn, Washington, USA and colleagues in India, are developing what they refer to as a "multilevel thrust filtration defending mechanism" to protect cloud computing environments against dDOS attacks. Their approach authenticates incoming requests and detects the different types of dDOS attacks at different levels to spot the most intensive attacks at an early stage and to then block unwanted traffic reaching the cloud service's data centers.

They reckon the total overhead costs to the server of integrating this filtering system would be a quarter of the cost of the overheads and downtime due to the dDOS if the tracking reaching the system is unfiltered. This, of course, does not take into account the loss of business revenues as customers and users are precluded from using the system effectively when a dDOS attack is under way.

More information: Iyengar, N.Ch.S.N., Ganapathy, G., Mogan Kumar, P.C and Abraham, A. (2014) 'A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment', *Int. J. Grid and Utility Computing*, Vol. 5, No. 4, pp.236–248.

Provided by Inderscience Publishers