Denial of Service

Nathan Pearce, 2012-15-10

Earlier in the year, the website of the Information Commissioner's Office (ico.gov.uk) was unavailable for a number of days after a denial of service (DoS) attack was launched against it. The ICO's servers were flooded with requests for information that they could not fulfil, eventually overloading them and bringing down the website. The attack was carried out by Anonymous, a 'hacktivist' group protesting against the Leveson Enquiry.

Denial of Service attacks have become a household name in the technology sector today. Quick and easy to mobilise, often making use of compromised PCs to launch 'distributed' denial of service attacks (DDoS) they have become effective at bringing many websites – including huge private sector brands Visa and Mastercard – to their knees.

Organisations should have an understanding of how to mitigate these issues. With hackers charging as little as $4 per hour for a DoS attack , this kind of attack has become cheaper than buying a take-away lunch.

The main techniques for dealing with DoS attacks rely on tracing the sources of the attack and blocking them. Security teams can identify the IP addresses from which the inbound traffic originates and block them – for example, sources which are attempting to make more than 800 connections per second. This can be done automatically.

Another solution to a DoS attack is to automatically determine whether the server request comes from a web browser, or whether it is generated by an automated script 'pinging' the server for information. Traditional web browsers are not designed to generate large numbers (i.e. up to a million per second) of server requests, so this is also a good way of separating genuine requests from DoS attacks.

There are more advanced DoS and DDoS techniques emerging, such as using compromised mobile phones with data access to also act as attackers. Hacker resources are also becoming considerable, making it more important to have a solution in place. According to one source the 'Low Orbit Ion Cannon' used by the Anonymous collective to bring down the ICO website consists of a network of 15,000 compromised PCs. 'akbot' another botnet used to generate DDoS attacks consists of over 1.3 million such devices.

Experts have suggested that in future, DDoS attacks may come from all kinds of devices, but also attack a variety of points simultaneously, for example, attacking a web app like an online banking application, but also the network and server that the application sits on: a 3DoS attack.

As we all know, prevention is better than cure. Putting measures in place which can deal with DoS attacks is a far more effective way of thwarting the hackers, and with threats rising in sophistication and persistence, digital defence needs to be on the agenda of all organisations today.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com