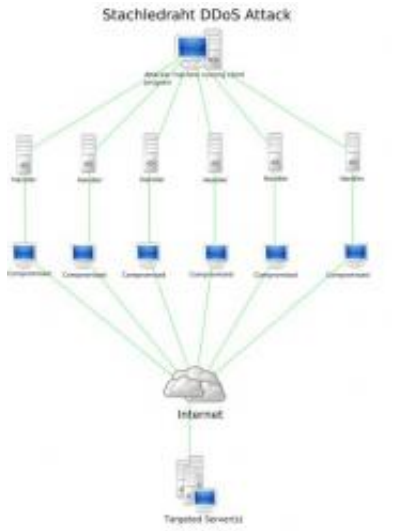
Hope on the horizon for victims of DDoS attacks

March 23 2011, by Bob Yirka



DDoS Stacheldraht Attack diagram. Everaldo Coelho/Wikipedia.

(PhysOrg.com) -- Recently, Yuri Gushin and Alex Behar, security experts with Radware, an Israeli security firm, gave a presentation at the Black Hat conference in Barcelona, Spain, and as part of their program showed what they've been working on to assist big website portals in fighting back against Distributed Denial of Service attacks (DDoS).

DDoS attacks are where one or more people use their own resources to cause as many computers as possible to try to access the services of a targeted website; flooding the server with requests to such an extent that

legitimate visitors are unable to gain access and do business. These kinds of attacks can happen either because there are enough people involved in a coordinated attack, or because those involved gain access to multiple other computers which they then direct to attack the chosen site.

DDoS attacks are not a new phenomena, but they have grown increasingly more pervasive in recent years as organizations, such as the infamous “Anonymous” gang of hackers, band together to forge new alliances, thereby increasing their ability to disrupt services. Such groups have come to use “botnets” or software robots to help them carry out their efforts. Botnets are created by implanting small pieces of code in as many unsuspecting computers as possible, then when a certain command is given, all of those computers start to harass the target; a giant army of software robots doing nothing more than creating a bottleneck that clogs up the web servers ability to carry out its job. The end result is legitimate users receiving messages saying they can’t access the site.

Gushin and Behar have devised a method of fighting back against such attacks that effectively deflects the barrage back on to the attacking computers, causing them to become so busy themselves that they eventually give up the attack. Their method works by taking advantage of the fact that the botnets aren’t human beings sitting behind computers running actual web pages. By placing code on the front end of the web server that demands those requesting entrance identify themselves automatically as a machine running HTML, or a scrip language such as Adobe Flash or JavaScript, legitimate users can be allowed in as their browsers automatically respond to the queries while those that aren’t running such protocols are never allowed in.

In another scenario, a web server can disrupt netbots by intentionally dropping a packet of data sent to them thus taking advantage of the Internet protocol that requires both sides in a conversation to reduce the amount of traffic they are sending, when an error occurs, which from the

netbots perspective, appears as a time out; the netbot then tries to overcome the obstacle by repeating the original request; which causes the whole sequence to run again, and again. In this scenario the netbot winds up becoming very busy while the web server goes on as if nothing has happened. Eventually the netbot will be forced to give up, or its presence will become known to the host, who will likely kill it.

In spite of these new advances in the war against the hackers, security experts such as Yuri Gushin and Alex Behar are not resting; they know it is only a matter of time before a way around the new defenses are found and they'll have to find a new way to stop them.

More information: www.radware.com/newsevents/pre … lease.aspx?id=182682