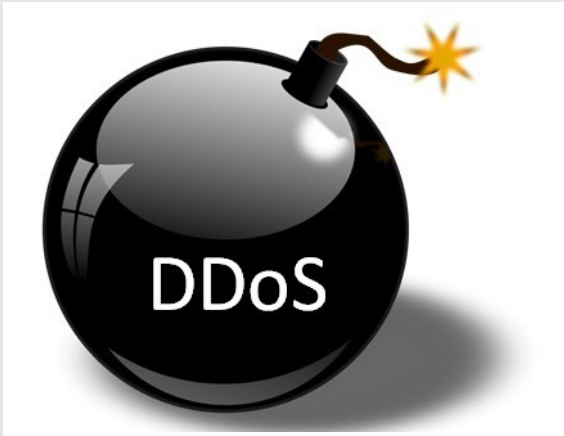
HackRead - Latest Cyber Crime - Information Security - Hacking News

Best Source for Latest Technology, Cyber Crime, Information Security & Hacking News

The 400Gbps largest DDoS attack has hit Europe using NTP Amplification

by **Waqas** on February 12, 2014 in **Cyber Crime News**

For temporary abandoning the services of the host that is connected to some internet, the most widely used and favorite method that is employed by hackers is the "Distributed Denial of Services DDoS". Almost all the big websites till date have fall victim to this attack at different times.



For the purpose of boosting these attacks, hackers since 2013 are using the Amplification Attack technique. The benefit with such tactics is that it obscures the attack's source, and enables the attack's bandwidth to be used for multiplying the size of such attack. The day before yesterday, unknown hackers have gone on to succeed in reaching newer heights of **DDoS** attack by targeting the anti-DDoS and content delivery firm known as Cloudfare. The attack reached 400Gbps and above at the peak of its traffic, striking the data servers of the company in Europe.

- **"Very big NTP reflection attack hitting us right now. Appears to be bigger than the #Spamhaus attack from last year. Mitigating," Cloudflare CEO Matthew Price said in a tweet. "Someone's got a big, new cannon. Start of ugly things to come,"**

This attack is recorded as the biggest in the history as it broke the previous

biggest record of 300Gbps. Hackers took the leverage from the weakness of NTP which is used for synchronizing the computer locks.

In the last few months, the frequency of tacks against the NTP have evidently increased. On the other hand, researchers have predicted from a long time that NTP has the potential to become an ideal DDoS tool and Vector for DDoS attacks someday. The trend has quite picked up in recent times and this has caused to create a lot of concerns for service provider and gaming websites.

US-CERT has recently given a warning in which it has listed out some UDP Protocols which have been identified as potential vectors of Amplification Attacks. They also include the NTP, DNS, NetBIOS, CharGEN, BitTorrent, QOTD, Quake Network, Kad, and the Protocol Steam Protocol.

The versions of the ntpd that have been prior to the version 4.2.7 have by default vulnerability in them. Therefore a simple recommendation is that the publically accessible version should be upgraded to at least the version 4.2.7. Therefore the mis-configured servers of NTP need to be cleaned up, or else the attacks will continue.

Comments

0 comments