Over 20Gbps DDoS attacks Now Become Common for Hackers

Article URL: http://thehackernews.com/2014/03/over-20gbps-ddos-attacks-now-become.html

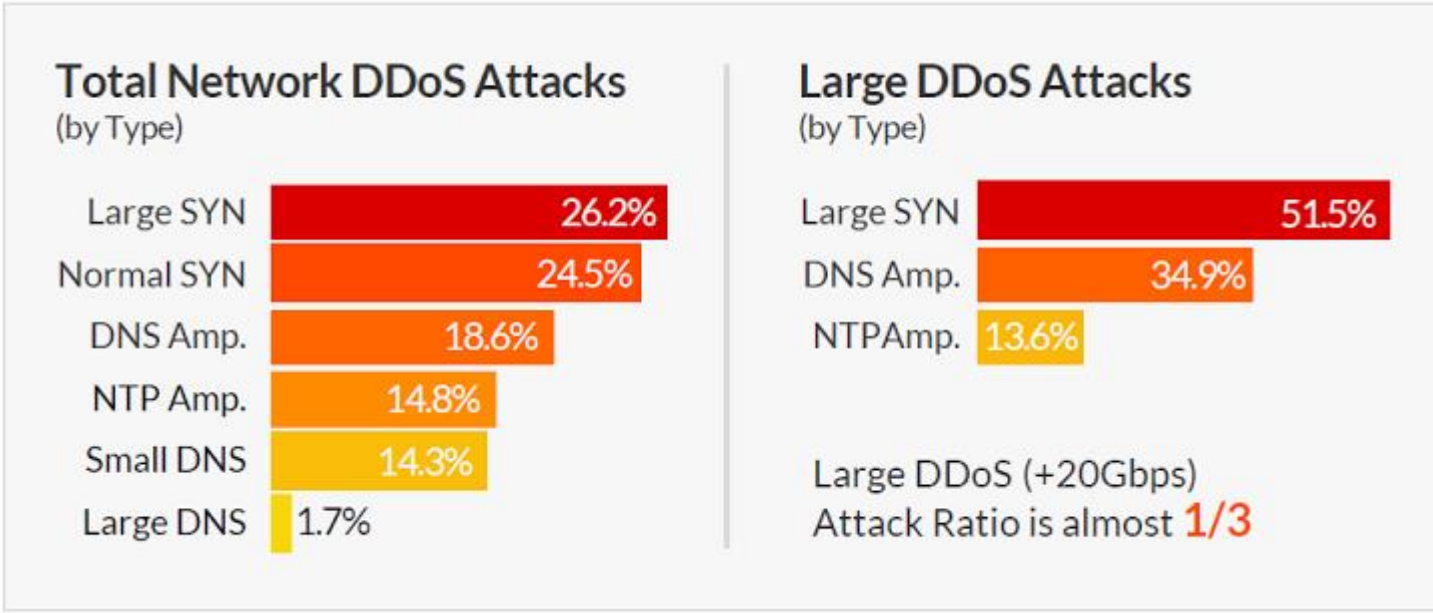
Sunday, March 30, 2014 by Swati Khandelwal

The Distributed Denial of Service (DDoS) attack has become more sophisticated and complex and therefore has become one of the favorite weapon for the cyber criminals to temporarily suspend the services of any host connected to the Internet and till now nearly every big site had been a victim of this attack, from WordPress to online game websites.

According to the new report released by a US based security solutions provider **Incapsula**, DDOS activities have become threefold since the start of the year 2013, pointing the key source of trash traffic to be the remotely controlled "*zombie army*" that can be used to flood various websites by DDoS attacks and other malicious activities.

The report site as "**DDOS Threat Landscape**", explains that almost one in every three DDoS attacks is above 20Gbps and 81% of attacks feature multiple vector threats.
The attackers are becoming more skillful at working around the network security and reusing their DDOS Botnets to attack multiple targets i.e. around 30% of the Botnets are flooding more than 50 targets a month.

"*As early as February 2013 we were able to track down a single-source 4Gbps attacking server, which – if amplified – could alone have generated over 200Gbps in attack traffic,"* the company said in its report.

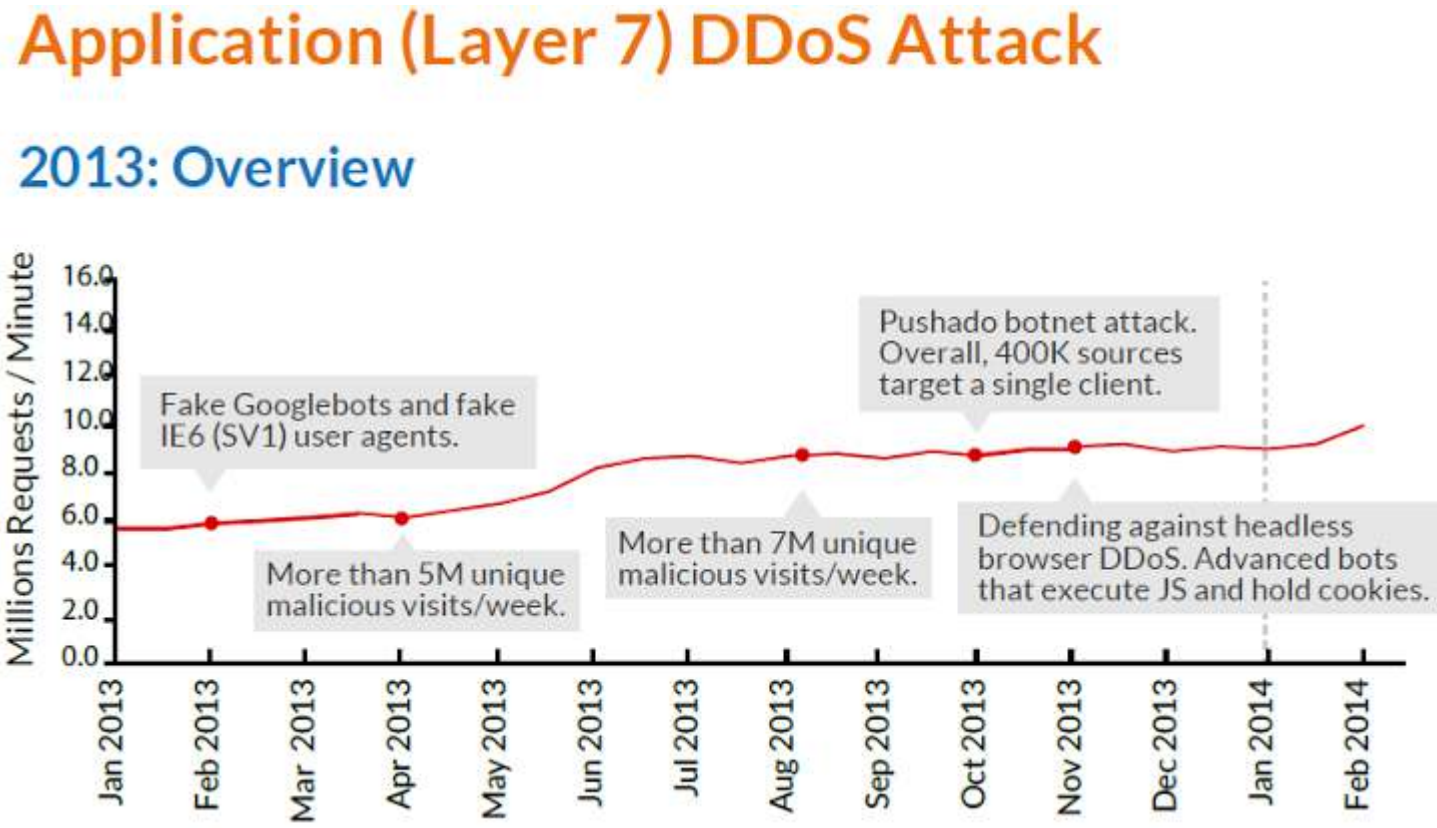


"With such available resources it is easy to explain the uptick in attack volume we saw over the course of the year."

Attackers are widely using two types of SYN flood attacks, i.e. regular SYN packets and large SYN packets. According to the report, 75% of all large scale network DDoS attacks that are peaking above 20Gbps are using both types of SYN flooding at same time.

However, currently amplification attacks became the most commonly used attack vector for large scale network DDoS attacks. During January and February of 2014 a significant increase in the number of NTP Amplification attacks were noticed.

Some statistics has also revealed an evolution of application DDOS attacks, where DDoS traffic is up by 240%, "*in almost 30% of all recorded sessions, the DDoS bots Incapsula encountered were able to accept and store cookies, while 0.8% of these bots could also execute JavaScript.*"



In terms of emerging threats, the report titled "*hit-and-run*" DDoS attacks, which were first documented in April 2013 and are the part of another parallel trend of attacks that were specifically designed to exploit vulnerabilities in DDoS protection services and human IT operators.

"*These attacks, which rely on frequent short bursts of traffic, are specifically designed to exploit the weakness of services that were designed for manual triggering (e.g., GRE tunneling to DNS re-routing),*" report reads. "*Hit-and-run attacks are now changing the face of anti-DDoS industry, pushing it towards always-on integrated solutions*."

Around one-third of all Botnets are located in India, China and Iran. The report ranks the United States as number five in the list of '*Top 10*' attacking countries.

In order to infiltrate systems bots are using spoofed user-agents, which help them to bypass low-level filtering solutions and about 46% of spoofed user-agents came from Chinese search engine Baidu, while nearly 12% mimicked Google.