NTP Amplification Attacks are on the rise?

Recently, there has been a lot of talk about DNS amplification attack incidents and the method behind them. The most notable case was the Spamhaus 300G attack. Since then, we have done detailed analysis and know exactly how the attack works. Amplification attacks are effective, and are driven by hackernomics – use the minimum amount of resources to cause the maximum amount of damage.

The problem is that very few entities, whether it is data centers, hosting providers, or even professional DDoS mitigation service providers have the capacity to handle such magnitude of attacks, let alone an enterprise or individual business. Unless there is the will and means available in the wider world working together to absorb this kind of attack, either through CDNs or Anti-DDoS mitigators to prevent victims' network infrastructures from simply bursting into flames at the onset of such attack, the ripple effect in terms of speed degradation and access latency will propagate around the whole world. No one will be spared.

However, if we think DNS amplification attack is difficult to handle, wait until we look into the NTP amplification attack.

As 300G attack traffic is already a tough nut to crack, what if the attack traffic peaks at 2T (2100G)? This disaster may come to reality once hackers use NTP servers for amplification attacks.

NTP is commonly used for system time synchronization. It is based on UDP transport (Port123) and provides certain commands issued by client to query for information.

A NTP client can issue a command "monlist" to query the IP addresses of the last 600 clients that has synchronized time with the targeted NTP server. In this way, just a small request packet can trigger sequencing UDP response packets containing active IP addresses and the other data.

The volume of the monlist response data is closely related to the number of the clients that communicate with NTP server. Hence a single request consists of 64-byte UDP packet can be magnified to 100 responses of 482 bytes each – a good 700x amplification. (Note: if we count the UDP packet size by payload only, 8 byte of request amplifies into 100x 440 bytes = 440*100/8=5500x)