DDoS NTP AMPLIFICATION ATTACKS: ARE YOU PRØTECTED?

Since the start of 2014 networks around the world have seen a huge increase in the number and size of DDoS attacks, specifically those caused by NTP Amplification attacks, but what are these attacks, what do they do and how can we stop them?

JUST HOW BIG IS THE PROBLEM?

Because the attack can be amplified up to 200 times, an attacker with access to a 1Gbps connection could in theory generate more than 200Gbps of DDoS traffic, which will give any operator or carrier some issues.

This is not just a theoretical risk, a recent attack in France used around 4500 NTP servers over more than 1000 networks to generate 400Gbps of DDoS traffic, it's impossible to know, but it is possible that this originated from a single server.

INCREASE IN FEB 2014

+807%

AVERAGE PEAK **PPS RATE**

2014: NETWORKS AROUND THE WORLD HAVE SEEN A HUGE INCREASE IN THE NUMBER AND SIZE OF DDOS ATTACKS

WHAT IS NTP AND WHY IS IT VULNERABLE?

NTP, Network Time Protocol, is used by all devices connected to the Internet to accurately set their clocks, computers, servers etc. Even mobile phones all use NTP servers to stay accurate. Its simplicity is what makes it vulnerable, it is a simple UDP-based protocol which in some cases requires no authentication to illicit a response, one such command is called MONLIST, which can be legitimately used for monitoring purposes.

MONLIST returns the addresses of up to the last 600 machines that the NTP server has interacted with, so a single request will generate a response which is much bigger, in fact it can be up to 200 times bigger, making it ideal for an amplification attack.

HOW DOES AN NTP AMPLIFICATION DDOS ATTACK WORK?

Firstly, the fact that no authentication is required to obtain a response means that the DDoS attacker can forge their address, so that the request looks like it originated from the intended victims machine. No checking is performed, so the NTP server simply responds to the forged source address and delivers the response to the target machine, this makes the attacker very hard to trace.

Next, the attacker will send forged requests to a large distributed number of servers across the internet and around the world, which can result in an overwhelming amount of traffic hitting the target, hence it becomes a Distributed Denial of Service attack.

With NTP the attack is in fact amplified, since the response is up to 200 times bigger than the request, so a very large attack can be created by a single machine, once amplified through a number of Distributed NTP servers. Amplification attacks of this nature, can turn a small amount of bandwidth coming from a small number of machines into huge attacks targeted on a specific device.

+371%

INCREASE IN TOTAL NTP AMPLIFICATION ATTACKS

RESPONSE

x200

AS A NETWORK PROVIDER, C4L TAKES ACTIVE PRECAUTIONS TO IDENTIFY AND THROTTLE DDOS TRAFFIC BEFORE IT CAN ENTER OUR NETWORK

PREVENTION IS BETTER THAN CURE

ESTIMATED THAT 93% OF THE WORLDS NTP SERVERS ARE NOW PROTECTED

The vulnerability in NTP servers has been addressed, but, server managers and network operators have to take action to 'patch' the software to prevent further attacks. It is estimated that 93% of the worlds NTP servers are now protected, and this number is improving constantly, but there is some way to go.

Network operators can easily check if there are 'open NTP servers', (NTP servers not yet protected with the latest software patch), running on their network by visiting the Open NTP Project: http://openntpproject.org. Some servers were actually shipped from the factory with this vulnerability, so everyone should perform some basic checks to ensure their NTP server is protected:

- Disable the MONLIST command
- Set your NTP server to client only mode
- Limit who can access your NTP server through a Firewall
- Upgrade to the latest version of software patch

If you need to run an NTP client or NTP server we would advise protecting it from the start using secure NTP Templates. C4L has already analysed its network and is working with customers and suppliers to ensure all potential vulnerabilities are addressed.

As a network provider C4L takes active precautions to identify and throttle DDoS traffic before it can enter our network, applying rate limiting and DDoS mitigation where appropriate. We test for Open NTP servers on a regular basis and deploy all new network equipment with BCP38 applied, to prevent spoofed packets from passing through the network.

HOW C4L CAN HELP

If you would like to find out more about DDOS NTP amplification attacks, how to accurately test and correctly configure your NTP, or simply want to know how to protect your business, please contact our team:

01202 299 799 www.C4L.co.uk

C4L, County Gates House, 300 Poole Road, Westbourne, Poole, Dorset. BH12 1AZ

Sources:
http://www.arbornetworks.com/asert/2014/03/ntp-attacks-continue-a-quick-look-at-traffic-over-the-past-few-months/
http://openntpproject.org
http://www.prolexic.com (Prolexic Quarterly Global DDoS Attack Report Q4 2013)

C4L

Colocation • Connectivity • Cloud • Communications