NTP amplification DDoS attack

Archived: 2026-04-05 18:20:37 UTC

What is a NTP amplification attack?

An NTP amplification attack is a reflection-based volumetric distributed denial-of-service (DDoS) attack in which an attacker exploits a Network Time Protocol (NTP) server functionality in order to overwhelm a targeted network or server with an amplified amount of UDP traffic, rendering the target and its surrounding infrastructure inaccessible to regular traffic.

How does a NTP amplification attack work?

All amplification attacks exploit a disparity in bandwidth cost between an attacker and the targeted web resource. When the disparity in cost is magnified across many requests, the resulting volume of traffic can disrupt network infrastructure. By sending small queries that result in large responses, the malicious user is able to get more from less. When multiplying this magnification by having each bot in a botnet make similar requests, the attacker is both obfuscated from detection and reaping the benefits of greatly increased attack traffic.

DNS flood attacks differ from DNS amplification attacks. Unlike DNS floods, DNS amplification attacks reflect and amplify traffic off unsecured DNS servers in order to hide the origin of the attack and increase its effectiveness. DNS amplification attacks use devices with smaller bandwidth connections to make numerous requests to unsecured DNS servers. The devices make many small requests for very large DNS records, but when making the requests, the attacker forges the return address to be that of the intended victim. The amplification allows the attacker to take out larger targets with only limited attack resources.

NTP amplification, much like DNS amplification, can be thought of in the context of a malicious teenager calling a restaurant and saying “I’ll have one of everything, please call me back and tell me my whole order.” When the restaurant asks for a callback number, the number given is the targeted victim’s phone number. The target then receives a call from the restaurant with a lot of information that they didn’t request.

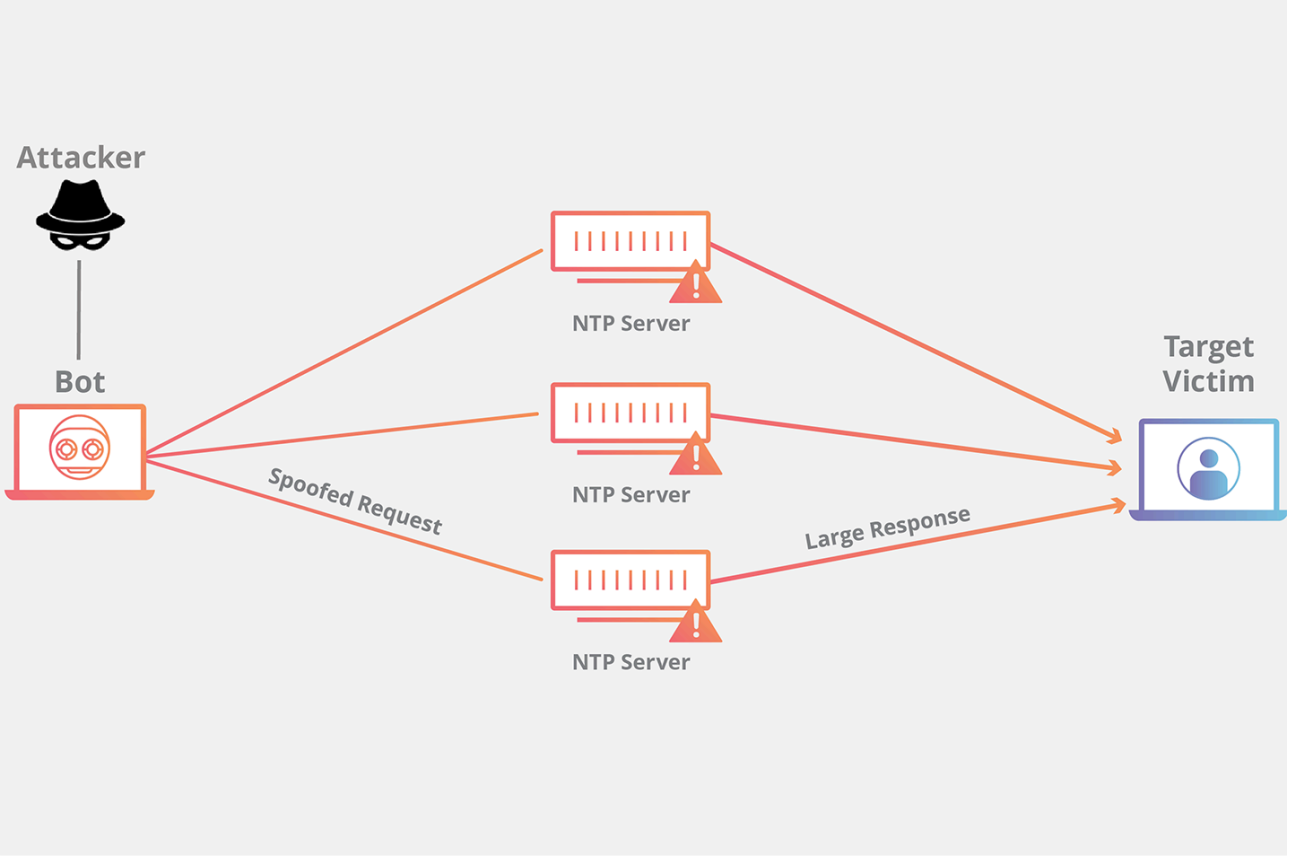
The Network Time Protocol is designed to allow internet connected devices to synchronize their internal clocks, and serves an important function in internet architecture. By exploiting the monlist command enabled on some NTP servers, an attacker is able to multiply their initial request traffic, resulting in a large response. This command is enabled by default on older devices, and responds with the last 600 source IP addresses of requests which have been made to the NTP server. The monlist request from a server with 600 addresses in its memory will be 206 times larger than the initial request. This means that an attacker with 1 GB of internet traffic can deliver a 200+ gigabyte attack - a massive increase in the resulting attack traffic.

An NTP amplification attack can be broken down into four steps:

1. The attacker uses a botnet to send UDP packets with spoofed IP addresses to a NTP server which has its monlist command enabled. The spoofed IP address on each packet points to the real IP address of the

victim.

2. Each UDP packet makes a request to the NTP server using its monlist command, resulting in a large response.
3. The server then responds to the spoofed address with the resulting data.
4. The IP address of the target receives the response and the surrounding network infrastructure becomes overwhelmed with the deluge of traffic, resulting in a denial-of-service.



As a result of the attack traffic looking like legitimate traffic coming from valid servers, mitigating this sort of attack traffic without blocking real NTP servers from legitimate activity is difficult. Because UDP packets do not require a handshake, the NTP server will send large responses to the targeted server without verifying that the request is authentic. These facts coupled with a built-in command, which by default sends a large response, makes NTP servers an excellent reflection source for DDoS amplification attacks.

How is a NTP amplification attack mitigated?

For an individual or company running a website or service, mitigation options are limited. This comes from the fact that the individual's server, while it might be the target, is not where the main effect of a volumetric attack is felt. Due to the high amount of traffic generated, the infrastructure surrounding the server feels the impact. The Internet Service Provider (ISP) or other upstream infrastructure providers may not be able to handle the incoming traffic without becoming overwhelmed. As a result, the ISP may blackhole all traffic to the targeted victim's IP address, protecting itself and taking the target's site off-line. Mitigation strategies, aside from offsite protective services like Cloudflare DDoS protection, are mostly preventative internet infrastructure solutions.

Disable monlist - reduce the number of NTP servers which support the monlist command.

A simple solution to patching the monlist vulnerability is to disable the command. All version of the NTP software prior to version 4.2.7 are vulnerable by default. By upgrading a NTP server to 4.2.7 or above, the command is disabled, patching the vulnerability. If upgrading is not possible, following the US-CERT instructions will allow a server's admin to make the necessary changes.

Source IP verification – stop spoofed packets leaving the network.

Because the UDP requests being sent by the attacker's botnet must have a source IP address spoofed to the victim's IP address, a key component in reducing the effectiveness of UDP-based amplification attacks is for internet service providers (ISPs) to reject any internal traffic with spoofed IP addresses. If a packet is being sent from inside the network with a source address that makes it appear like it originated outside the network, it's likely a spoofed packet and can be dropped. Cloudflare highly recommends that all providers implement ingress filtering, and at times will reach out to ISPs who are unknowingly taking part in DDoS attacks (in violation of BCP38) and help them realize their vulnerability.

The combination of disabling monlist on NTP servers and implementing ingress filtering on networks which presently allow IP spoofing is an effective way to stop this type of attack before it reaches its intended network.

How does Cloudflare mitigate NTP amplification attacks?

With a properly configured firewall and sufficient network capacity (which isn't always easy to come by unless you are the size of Cloudflare), it's trivial to block reflection attacks such as NTP amplification attacks. Although the attack will target a single IP address, our Anycast network will scatter all attack traffic to the point where it is no longer disruptive. Cloudflare is able to use our advantage of scale to distribute the weight of the attack across many Data Centers, balancing the load so that service is never interrupted and the attack never overwhelms the targeted server's infrastructure. During a recent six-month window, our DDoS mitigation system "Gatebot" detected 6,329 simple reflection attacks (that's one every 40 minutes), and the network successfully mitigated all of them. Learn more about Cloudflare's advanced DDoS Protection.
