DNS amplification DDoS attack

Archived: 2026-04-05 16:01:30 UTC

What is a DNS amplification attack?

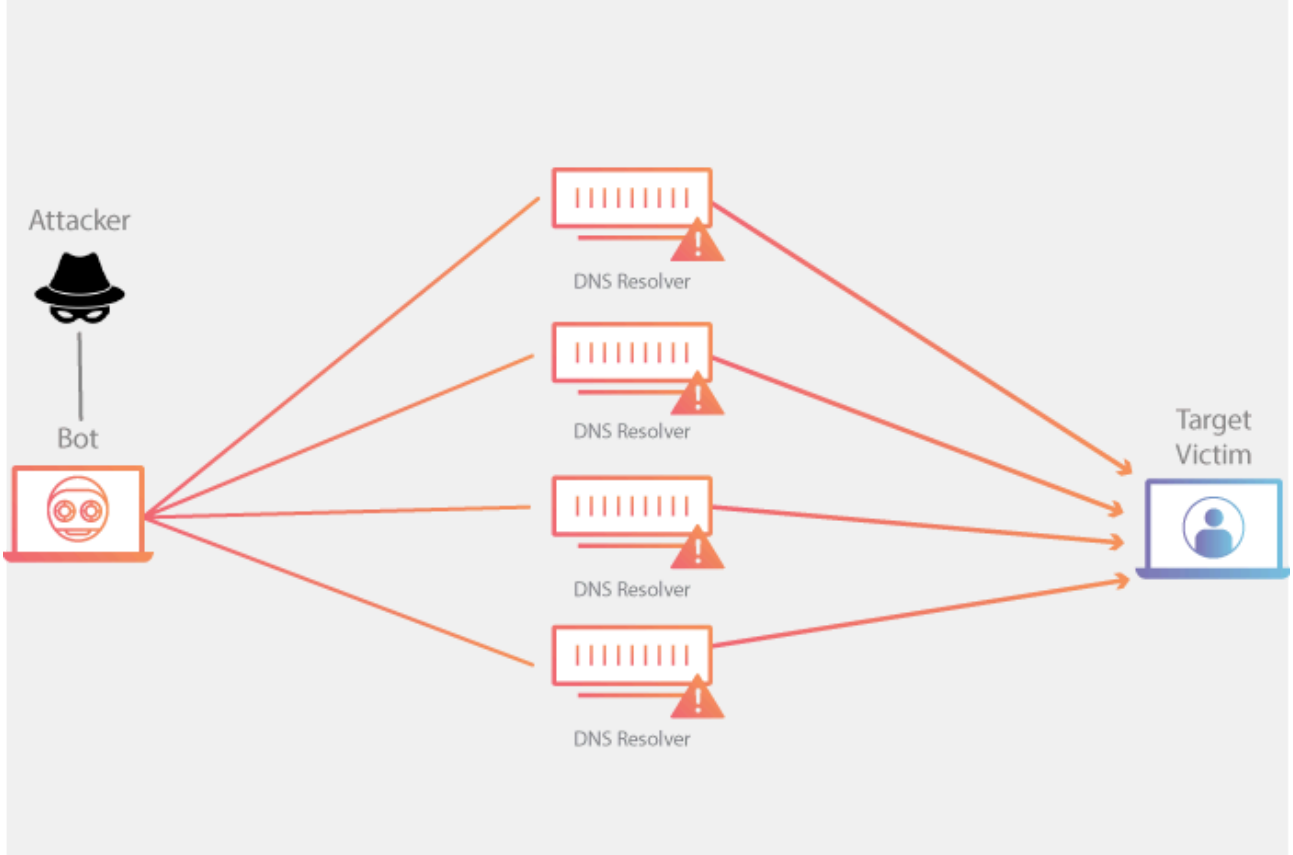
This DDoS attack is a reflection-based volumetric distributed denial-of-service (DDoS) attack in which an attacker leverages the functionality of open DNS resolvers in order to overwhelm a target server or network with an amplified amount of traffic, rendering the server and its surrounding infrastructure inaccessible.

How does a DNS amplification attack work?

All amplification attacks exploit a disparity in bandwidth consumption 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. By 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.

A single bot in a DNS amplification attack 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.

As a result of each bot making requests to open DNS resolvers with a spoofed IP address, which has been changed to the real source IP address of the targeted victim, the target then receives a response from the DNS resolvers. In order to create a large amount of traffic, the attacker structures the request in a way that generates as large a response from the DNS resolvers as possible. As a result, the target receives an amplification of the attacker’s initial traffic, and their network becomes clogged with the spurious traffic, causing a denial-of-service.



A DNS amplification can be broken down into four steps:

1. The attacker uses a compromised endpoint to send UDP packets with spoofed IP addresses to a DNS recursor. The spoofed address on the packets points to the real IP address of the victim.
2. Each one of the UDP packets makes a request to a DNS resolver, often passing an argument such as "ANY" in order to receive the largest response possible.
3. After receiving the requests, the DNS resolver, which is trying to be helpful by responding, sends a large response to the spoofed IP address.
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.

While a few requests is not enough to take down network infrastructure, when this sequence is multiplied across multiple requests and DNS resolvers, the amplification of data the target receives can be substantial. Explore more technical details on reflection attacks.

How is a DNS 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.

Reduce the total number of open DNS resolvers

An essential component of DNS amplification attacks is access to open DNS resolvers. By having poorly configured DNS resolvers exposed to the Internet, all an attacker needs to do to utilize a DNS resolver is to discover it. Ideally, DNS resolvers should only provide their services to devices that originate within a trusted domain. In the case of reflection based attacks, the open DNS resolvers will respond to queries from anywhere on the Internet, allowing the potential for exploitation. Restricting a DNS resolver so that it will only respond to queries from trusted sources makes the server a poor vehicle for any type of amplification attack.

Source IP verification – stop spoofed packets leaving 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 and help them realize their vulnerability.

How does Cloudflare mitigate DNS 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 DNS 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.
