Network Denial of Service: Reflection Amplification, Sub-technique T1498.002 - Enterprise

Archived: 2026-04-05 18:08:22 UTC

Adversaries may attempt to cause a denial of service (DoS) by reflecting a high-volume of network traffic to a target. This type of Network DoS takes advantage of a third-party server intermediary that hosts and will respond to a given spoofed source IP address. This third-party server is commonly termed a reflector. An adversary accomplishes a reflection attack by sending packets to reflectors with the spoofed address of the victim. Similar to Direct Network Floods, more than one system may be used to conduct the attack, or a botnet may be used. Likewise, one or more reflectors may be used to focus traffic on the target.[1] This Network DoS attack may also reduce the availability and functionality of the targeted system(s) and network.

Reflection attacks often take advantage of protocols with larger responses than requests in order to amplify their traffic, commonly known as a Reflection Amplification attack. Adversaries may be able to generate an increase in volume of attack traffic that is several orders of magnitude greater than the requests sent to the amplifiers. The extent of this increase will depending upon many variables, such as the protocol in question, the technique used, and the amplifying servers that actually produce the amplification in attack volume. Two prominent protocols that have enabled Reflection Amplification Floods are DNS[2] and NTP[3], though the use of several others in the wild have been documented.[4] In particular, the memcache protocol showed itself to be a powerful protocol, with amplification sizes up to 51,200 times the requesting packet.[5]

Source: https://attack.mitre.org/techniques/T1498/002