# TTP Detail – T1498.001

## TTP Information

Name: Direct Network Flood

Description: Adversaries may attempt to cause a denial of service (DoS) by directly sending a high-volume of network traffic to a target. This DoS attack may also reduce the availability and functionality of the targeted system(s) and network. [Direct Network Flood](https://attack.mitre.org/techniques/T1498/001)s are when one or more systems are used to send a high-volume of network packets towards the targeted service's network. Almost any network protocol may be used for flooding. Stateless protocols such as UDP or ICMP are commonly used but stateful protocols such as TCP can be used as well.

Botnets are commonly used to conduct network flooding attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global Internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an attack. In some of the worst cases for distributed DoS (DDoS), so many systems are used to generate the flood that each one only needs to send out a small amount of traffic to produce enough volume to saturate the target network. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS flooding attacks, such as the 2012 series of incidents that targeted major US banks.(Citation: USNYAG IranianBotnet March 2016)

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## Kill Chain Phases

**•** mitre-attack: impact