# TTP Detail – T1499.002

## TTP Information

Name: Service Exhaustion Flood

Description: Adversaries may target the different network services provided by systems to conduct a denial of service (DoS). Adversaries often target the availability of DNS and web services, however others have been targeted as well.(Citation: Arbor AnnualDoSreport Jan 2018) Web server software can be attacked through a variety of means, some of which apply generally while others are specific to the software being used to provide the service.

One example of this type of attack is known as a simple HTTP flood, where an adversary sends a large number of HTTP requests to a web server to overwhelm it and/or an application that runs on top of it. This flood relies on raw volume to accomplish the objective, exhausting any of the various resources required by the victim software to provide the service.(Citation: Cloudflare HTTPflood)

Another variation, known as a SSL renegotiation attack, takes advantage of a protocol feature in SSL/TLS. The SSL/TLS protocol suite includes mechanisms for the client and server to agree on an encryption algorithm to use for subsequent secure connections. If SSL renegotiation is enabled, a request can be made for renegotiation of the crypto algorithm. In a renegotiation attack, the adversary establishes a SSL/TLS connection and then proceeds to make a series of renegotiation requests. Because the cryptographic renegotiation has a meaningful cost in computation cycles, this can cause an impact to the availability of the service when done in volume.(Citation: Arbor SSLDoS April 2012)

## Threat-Mapped Scoring

Score: 1.9

Priority: P3 - Important (Medium)

## Kill Chain Phases

**•** mitre-attack: impact