# TTP Detail – T1568.001

## TTP Information

Name: Fast Flux DNS

Description: Adversaries may use Fast Flux DNS to hide a command and control channel behind an array of rapidly changing IP addresses linked to a single domain resolution. This technique uses a fully qualified domain name, with multiple IP addresses assigned to it which are swapped with high frequency, using a combination of round robin IP addressing and short Time-To-Live (TTL) for a DNS resource record.(Citation: MehtaFastFluxPt1)(Citation: MehtaFastFluxPt2)(Citation: Fast Flux - Welivesecurity)

The simplest, "single-flux" method, involves registering and de-registering an addresses as part of the DNS A (address) record list for a single DNS name. These registrations have a five-minute average lifespan, resulting in a constant shuffle of IP address resolution.(Citation: Fast Flux - Welivesecurity)

In contrast, the "double-flux" method registers and de-registers an address as part of the DNS Name Server record list for the DNS zone, providing additional resilience for the connection. With double-flux additional hosts can act as a proxy to the C2 host, further insulating the true source of the C2 channel.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: command-and-control

## Malware

* Amadey
* gh0st RAT
* njRAT

## APTs (Intrusion Sets)

* Gamaredon Group
* TA505
* menuPass