# TTP Detail – T1568

## TTP Information

Name: Dynamic Resolution

Description: Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations. This may be achieved by using malware that shares a common algorithm with the infrastructure the adversary uses to receive the malware's communications. These calculations can be used to dynamically adjust parameters such as the domain name, IP address, or port number the malware uses for command and control.

Adversaries may use dynamic resolution for the purpose of [Fallback Channels](https://attack.mitre.org/techniques/T1008). When contact is lost with the primary command and control server malware may employ dynamic resolution as a means to reestablishing command and control.(Citation: Talos CCleanup 2017)(Citation: FireEye POSHSPY April 2017)(Citation: ESET Sednit 2017 Activity)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* Bisonal
* Gelsemium
* Maze
* NETEAGLE
* RTM
* SUNBURST
* Tomiris

## Tools

* AsyncRAT

## APTs (Intrusion Sets)

* APT29
* BITTER
* Gamaredon Group
* RedEcho
* TA2541
* Transparent Tribe