# TTP Detail – T1583.002

## TTP Information

Name: DNS Server

Description: Adversaries may set up their own Domain Name System (DNS) servers that can be used during targeting. During post-compromise activity, adversaries may utilize DNS traffic for various tasks, including for Command and Control (ex: [Application Layer Protocol](https://attack.mitre.org/techniques/T1071)). Instead of hijacking existing DNS servers, adversaries may opt to configure and run their own DNS servers in support of operations.

By running their own DNS servers, adversaries can have more control over how they administer server-side DNS C2 traffic ([DNS](https://attack.mitre.org/techniques/T1071/004)). With control over a DNS server, adversaries can configure DNS applications to provide conditional responses to malware and, generally, have more flexibility in the structure of the DNS-based C2 channel.(Citation: Unit42 DNS Mar 2019)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: resource-development

## APTs (Intrusion Sets)

* Axiom
* HEXANE
* Sea Turtle