# TTP Detail – T1584.002

## TTP Information

Name: DNS Server

Description: Adversaries may compromise third-party 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 setting up their own DNS servers, adversaries may compromise third-party DNS servers in support of operations.  
  
By compromising DNS servers, adversaries can alter DNS records. Such control can allow for redirection of an organization's traffic, facilitating Collection and Credential Access efforts for the adversary.(Citation: Talos DNSpionage Nov 2018)(Citation: FireEye DNS Hijack 2019) Additionally, adversaries may leverage such control in conjunction with [Digital Certificates](https://attack.mitre.org/techniques/T1588/004) to redirect traffic to adversary-controlled infrastructure, mimicking normal trusted network communications.(Citation: FireEye DNS Hijack 2019)(Citation: Crowdstrike DNS Hijack 2019) Adversaries may also be able to silently create subdomains pointed at malicious servers without tipping off the actual owner of the DNS server.(Citation: CiscoAngler)(Citation: Proofpoint Domain Shadowing)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## APTs (Intrusion Sets)

* LAPSUS$
* Sea Turtle