# TTP Detail – T1584.004

## TTP Information

Name: Server

Description: Adversaries may compromise third-party servers that can be used during targeting. Use of servers allows an adversary to stage, launch, and execute an operation. During post-compromise activity, adversaries may utilize servers for various tasks, including for Command and Control.(Citation: TrendMicro EarthLusca 2022) Instead of purchasing a [Server](https://attack.mitre.org/techniques/T1583/004) or [Virtual Private Server](https://attack.mitre.org/techniques/T1583/003), adversaries may compromise third-party servers in support of operations.

Adversaries may also compromise web servers to support watering hole operations, as in [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), or email servers to support [Phishing](https://attack.mitre.org/techniques/T1566) operations.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## APTs (Intrusion Sets)

* APT16
* Daggerfly
* Dragonfly
* Earth Lusca
* Indrik Spider
* Lazarus Group
* Leviathan
* Sandworm Team
* Turla
* Volt Typhoon