# TTP Detail – T1584

## TTP Information

Name: Compromise Infrastructure

Description: Adversaries may compromise third-party infrastructure that can be used during targeting. Infrastructure solutions include physical or cloud servers, domains, network devices, and third-party web and DNS services. Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it during other phases of the adversary lifecycle.(Citation: Mandiant APT1)(Citation: ICANNDomainNameHijacking)(Citation: Talos DNSpionage Nov 2018)(Citation: FireEye EPS Awakens Part 2) Additionally, adversaries may compromise numerous machines to form a botnet they can leverage.

Use of compromised infrastructure allows adversaries to stage, launch, and execute operations. Compromised infrastructure can help adversary operations blend in with traffic that is seen as normal, such as contact with high reputation or trusted sites. For example, adversaries may leverage compromised infrastructure (potentially also in conjunction with [Digital Certificates](https://attack.mitre.org/techniques/T1588/004)) to further blend in and support staged information gathering and/or [Phishing](https://attack.mitre.org/techniques/T1566) campaigns.(Citation: FireEye DNS Hijack 2019) Adversaries may also compromise numerous machines to support [Proxy](https://attack.mitre.org/techniques/T1090) and/or proxyware services or to form a botnet.(Citation: amnesty\_nso\_pegasus)(Citation: Sysdig Proxyjacking) Additionally, adversaries may compromise infrastructure residing in close proximity to a target in order to gain [Initial Access](https://attack.mitre.org/tactics/TA0001) via [Wi-Fi Networks](https://attack.mitre.org/techniques/T1669).(Citation: Nearest Neighbor Volexity)

By using compromised infrastructure, adversaries may enable follow-on malicious operations. Prior to targeting, adversaries may also compromise the infrastructure of other adversaries.(Citation: NSA NCSC Turla OilRig)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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