# TTP Detail – T1583.006

## TTP Information

Name: Web Services

Description: Adversaries may register for web services that can be used during targeting. A variety of popular websites exist for adversaries to register for a web-based service that can be abused during later stages of the adversary lifecycle, such as during Command and Control ([Web Service](https://attack.mitre.org/techniques/T1102)), [Exfiltration Over Web Service](https://attack.mitre.org/techniques/T1567), or [Phishing](https://attack.mitre.org/techniques/T1566). Using common services, such as those offered by Google, GitHub, or Twitter, makes it easier for adversaries to hide in expected noise.(Citation: FireEye APT29)(Citation: Hacker News GitHub Abuse 2024) By utilizing a web service, adversaries can make it difficult to physically tie back operations to them.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## APTs (Intrusion Sets)

* APT17
* APT28
* APT29
* APT32
* Confucius
* Earth Lusca
* FIN7
* HAFNIUM
* IndigoZebra
* Kimsuky
* Lazarus Group
* LazyScripter
* Magic Hound
* MuddyWater
* POLONIUM
* Saint Bear
* TA2541
* TA578
* Turla
* ZIRCONIUM