# TTP Detail – T1593.003

## TTP Information

Name: Code Repositories

Description: Adversaries may search public code repositories for information about victims that can be used during targeting. Victims may store code in repositories on various third-party websites such as GitHub, GitLab, SourceForge, and BitBucket. Users typically interact with code repositories through a web application or command-line utilities such as git.

Adversaries may search various public code repositories for various information about a victim. Public code repositories can often be a source of various general information about victims, such as commonly used programming languages and libraries as well as the names of employees. Adversaries may also identify more sensitive data, including accidentally leaked credentials or API keys.(Citation: GitHub Cloud Service Credentials) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [Valid Accounts](https://attack.mitre.org/techniques/T1078) or [Phishing](https://attack.mitre.org/techniques/T1566)).

\*\*Note:\*\* This is distinct from [Code Repositories](https://attack.mitre.org/techniques/T1213/003), which focuses on [Collection](https://attack.mitre.org/tactics/TA0009) from private and internally hosted code repositories.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: reconnaissance

## APTs (Intrusion Sets)

* HAFNIUM
* LAPSUS$