# TTP Detail – T1594

## TTP Information

Name: Search Victim-Owned Websites

Description: Adversaries may search websites owned by the victim for information that can be used during targeting. Victim-owned websites may contain a variety of details, including names of departments/divisions, physical locations, and data about key employees such as names, roles, and contact info (ex: [Email Addresses](https://attack.mitre.org/techniques/T1589/002)). These sites may also have details highlighting business operations and relationships.(Citation: Comparitech Leak)

Adversaries may search victim-owned websites to gather actionable information. Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Trusted Relationship](https://attack.mitre.org/techniques/T1199) or [Phishing](https://attack.mitre.org/techniques/T1566)).

In addition to manually browsing the website, adversaries may attempt to identify hidden directories or files that could contain additional sensitive information or vulnerable functionality. They may do this through automated activities such as [Wordlist Scanning](https://attack.mitre.org/techniques/T1595/003), as well as by leveraging files such as sitemap.xml and robots.txt.(Citation: Perez Sitemap XML 2023)(Citation: Register Robots TXT 2015)

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: reconnaissance

## APTs (Intrusion Sets)

* EXOTIC LILY
* Kimsuky
* Sandworm Team
* Silent Librarian
* TA578
* Volt Typhoon