# TTP Detail – T1595.003

## TTP Information

Name: Wordlist Scanning

Description: Adversaries may iteratively probe infrastructure using brute-forcing and crawling techniques. While this technique employs similar methods to [Brute Force](https://attack.mitre.org/techniques/T1110), its goal is the identification of content and infrastructure rather than the discovery of valid credentials. Wordlists used in these scans may contain generic, commonly used names and file extensions or terms specific to a particular software. Adversaries may also create custom, target-specific wordlists using data gathered from other Reconnaissance techniques (ex: [Gather Victim Org Information](https://attack.mitre.org/techniques/T1591), or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).

For example, adversaries may use web content discovery tools such as Dirb, DirBuster, and GoBuster and generic or custom wordlists to enumerate a website’s pages and directories.(Citation: ClearSky Lebanese Cedar Jan 2021) This can help them to discover old, vulnerable pages or hidden administrative portals that could become the target of further operations (ex: [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190) or [Brute Force](https://attack.mitre.org/techniques/T1110)).

As cloud storage solutions typically use globally unique names, adversaries may also use target-specific wordlists and tools such as s3recon and GCPBucketBrute to enumerate public and private buckets on cloud infrastructure.(Citation: S3Recon GitHub)(Citation: GCPBucketBrute) Once storage objects are discovered, adversaries may leverage [Data from Cloud Storage](https://attack.mitre.org/techniques/T1530) to access valuable information that can be exfiltrated or used to escalate privileges and move laterally.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: reconnaissance

## APTs (Intrusion Sets)

* APT41
* Volatile Cedar