# TTP Detail – T1596.004

## TTP Information

Name: CDNs

Description: Adversaries may search content delivery network (CDN) data about victims that can be used during targeting. CDNs allow an organization to host content from a distributed, load balanced array of servers. CDNs may also allow organizations to customize content delivery based on the requestor’s geographical region.

Adversaries may search CDN data to gather actionable information. Threat actors can use online resources and lookup tools to harvest information about content servers within a CDN. Adversaries may also seek and target CDN misconfigurations that leak sensitive information not intended to be hosted and/or do not have the same protection mechanisms (ex: login portals) as the content hosted on the organization’s website.(Citation: DigitalShadows CDN) Information from these sources may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) or [Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)), and/or initial access (ex: [Drive-by Compromise](https://attack.mitre.org/techniques/T1189)).

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: reconnaissance