# TTP Detail – T1608.006

## TTP Information

Name: SEO Poisoning

Description: Adversaries may poison mechanisms that influence search engine optimization (SEO) to further lure staged capabilities towards potential victims. Search engines typically display results to users based on purchased ads as well as the site’s ranking/score/reputation calculated by their web crawlers and algorithms.(Citation: Atlas SEO)(Citation: MalwareBytes SEO)

To help facilitate [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), adversaries may stage content that explicitly manipulates SEO rankings in order to promote sites hosting their malicious payloads (such as [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)) within search engines. Poisoning SEO rankings may involve various tricks, such as stuffing keywords (including in the form of hidden text) into compromised sites. These keywords could be related to the interests/browsing habits of the intended victim(s) as well as more broad, seasonably popular topics (e.g. elections, trending news).(Citation: ZScaler SEO)(Citation: Atlas SEO)

In addition to internet search engines (such as Google), adversaries may also aim to manipulate specific in-site searches for developer platforms (such as GitHub) to deceive users towards [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) lures. In-site searches will rank search results according to their own algorithms and metrics such as popularity(Citation: Chexmarx-seo) which may be targeted and gamed by malicious actors.(Citation: Checkmarx-oss-seo)

Adversaries may also purchase or plant incoming links to staged capabilities in order to boost the site’s calculated relevance and reputation.(Citation: MalwareBytes SEO)(Citation: DFIR Report Gootloader)

SEO poisoning may also be combined with evasive redirects and other cloaking mechanisms (such as measuring mouse movements or serving content based on browser user agents, user language/localization settings, or HTTP headers) in order to feed SEO inputs while avoiding scrutiny from defenders.(Citation: ZScaler SEO)(Citation: Sophos Gootloader)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## APTs (Intrusion Sets)

* Mustard Tempest