SEO Poisoning

What is SEO poisoning?

Search Engine Optimization (SEO) poisoning is a tactic in which attackers manipulate search engine results to promote malicious websites. By using search engine optimization techniques, threat actors can force harmful links higher in search rankings, making them appear legitimate, trustworthy, and popular. When victims click on these results, they are often led to malicious sites that deliver a wide range of different malware or act as credential harvesters. SEO poisoning is particularly dangerous because it leverages the trust users place in search engines to deliver safe content.
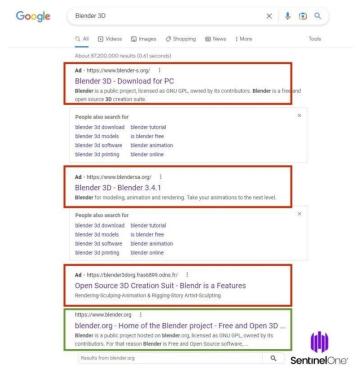
Who does SEO poisoning target?

Attackers leveraging SEO poisoning typically focus on topics with widespread public interest or high search volume to increase the likelihood of luring users into malicious sites. They manipulate search engine rankings to promote compromised websites that align with current trends, such as breaking news, urgent events, or commonly sought-after services.

Threat actors also might focus on SEO poisoning for specific software or tools used in corporate or enterprise environments that are targets for ransomware or data extortion. Threat actors may even use SEO poisoning tactics to target a specific entity and its employees.

SEO poisoning campaigns that tend to be more impactful often coincide with the presence of a zero-day or unpatched vulnerability that the threat actor's malware is designed to exploit.

Example of SEO poisoning

Source: https://www.techrepublic.com/article/seo-poisoning-brand-reputation/