HC3 Analyst Note

June 22, 2023 TLP:CLEAR Report: 202306221200

SEO Poisoning

Executive Summary

Search engine optimization (SEO) poisoning, considered a type of malvertising (malicious advertising), is a technique used by threat actors to increase the prominence of their malicious websites, making them look more authentic to consumers. SEO poisoning tricks the human mind, which naturally assumes the top hits are the most credible, and is very effective when people fail to look closely at their search results. This can lead to credential theft, malware infections, and financial losses. As more organizations utilize search engines and healthcare continues to digitally transform, SEO poisoning is becoming a larger security threat. HC3 has observed this attack method being used recently and frequently against the U.S. Healthcare and Public Health (HPH) sector.

What is SEO Poisoning?

SEO poisoning attacks consist of altering search engine results so that the first advertised links actually lead to attacker-controlled sites, generally to infect visitors with malware or to attract more people using ad fraud. A user who does not read the URL (web address) closely or is unsure of the exact URL of the software might click on any of those attacker-controlled domains, which could result in a compromise.

Threat actors may even use targeted types of SEO poisoning, like spear-phishing, to go after specific users, like IT administrators. The technique enables attackers to target and customize their attacks to specific audiences, making them more challenging to identify and defend against.

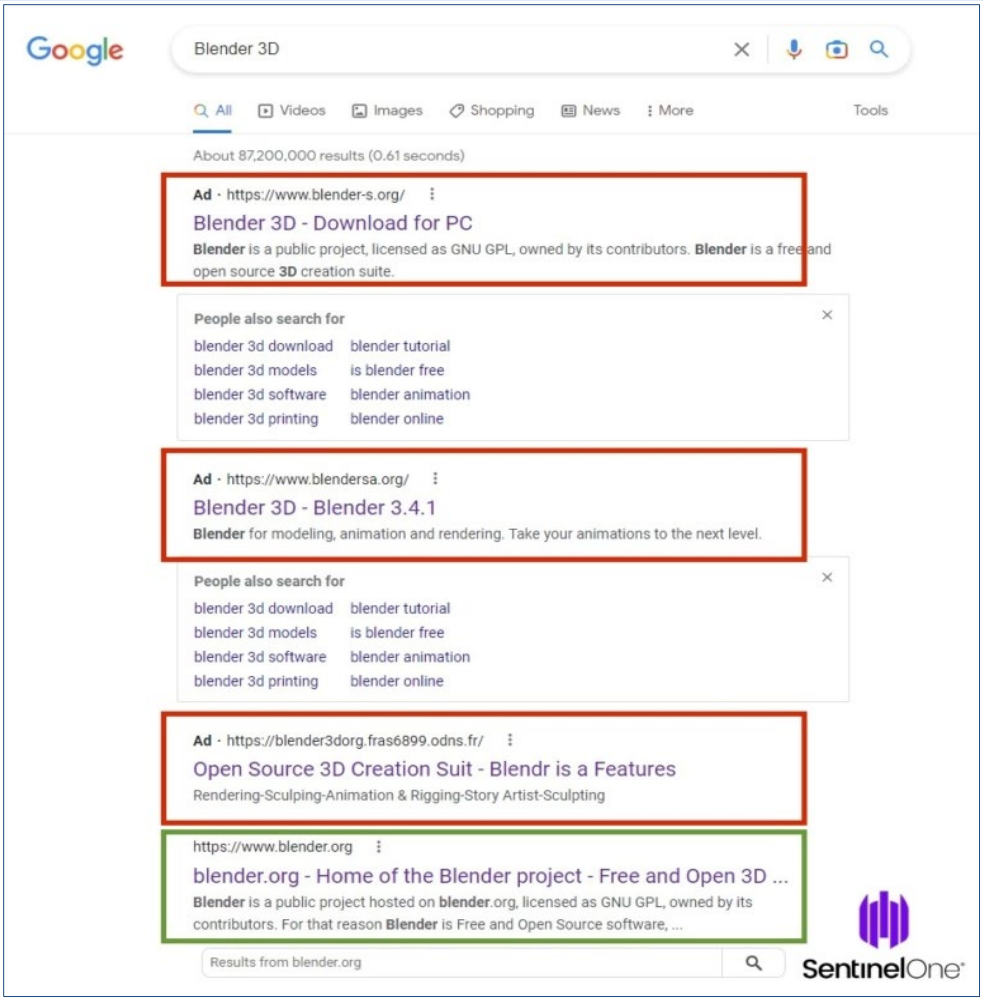
How SEO Poisoning Works

Malicious actors use a variety of techniques to accomplish SEO poisoning. One common method is typosquatting, which targets users who might open their browser and input a website address that has an inadvertent typo or click on a link with a misspelled URL. To exploit these minor user errors, attackers register domain names similar to legitimate ones.

An example of this would be a user searching a keyword in their web browser. The user may hit the first result without looking too closely at the URL—which can contain misspellings like "Goggle" instead of “Google” or characters that look similar like “1” instead of “l”—and be redirected to a fake website where they are prompted to download malware-infected files.

HC3 Analyst Note

June 22, 2023 TLP:CLEAR Report: 202306221200



An example of SEO poisoning.
Source: SentinelOne

Typosquatting domains are often featured at the top of the search results, making it likely that users will click on them. This is where blackhat SEO—which refers to unethical tactics website owners use to boost search engine ranks, such as keyword stuffing, cloaking, search ranking manipulation, and using private link networks—comes in.

- **Keyword stuffing**: Cramming irrelevant keywords into a webpage's text, meta tags, or other portions of the website to mislead search engine algorithms into giving the website a higher ranking.
- **Cloaking**: Presenting search engine crawlers with different material than what's displayed to the user when the link is clicked. This method influences search engine rankings by displaying favorable information to crawlers while displaying irrelevant content to users.
- **Manipulating search ranking**: Artificially increasing a website's click-through rate to boost its ranking in search engines. This method utilizes bots or humans to search for keywords and generate fake clicks for a particular website.
- **Using private link networks**: Creating a group of unrelated websites and connecting them to each other, resulting in a network of backlinks to a main website. This is also a method of boosting search engine results artificially, as it seeks to imitate legitimate link-building practices.

HC3 Analyst Note

June 22, 2023 TLP:CLEAR Report: 202306221200

Detecting & Preventing SEO Poisoning

Detecting and preventing SEO poisoning can be difficult, but organizations can better prepare themselves by:

- Implementing typosquatting detection procedures using Digital Risk Monitoring tools. Organizations should carefully check every new domain that is registered on the Internet that contains similarities with any of their brands or names. As attackers often register domain names that are very similar to the legitimate ones, it is possible to detect them quickly in most cases, immediately analyze the situation, and take action to mitigate the risk. Tips and resources for reporting fraud to hosting companies and/or law enforcement can be found here.
- Another method to detect malicious URLs is through the usage of indicators of compromise (IOC) lists. IOC lists can provide information of suspicious website behavior, anomalous search engine rankings, phishing attempts, unexpected changes in website traffic, and suspicious content. The lists can be used as watchlists or blocklists for preemptive detection or blocking.
- Upgrading security software and establishing rigorous web filtering procedures.
- User Security Training and Awareness: Organizations may lower the chances of falling prey to these attacks by training staff on safe browsing practices, phishing awareness, and effective endpoint security measures.

References

Breaking Down the SEO Poisoning Attack | How Attackers Are Hijacking Search Results
https://www.sentinelone.com/blog/breaking-down-the-seo-poisoning-attack-how-attackers-are-hijacking-search-results/

Recent rise in SEO poisoning attacks compromise brand reputations
https://www.techrepublic.com/article/seo-poisoning-brand-reputation/

SEO Poisoning, Cobalt Strike Abuse, Emotet Continue to Threaten Healthcare Cybersecurity
https://healthitsecurity.com/news/seo-poisoning-cobalt-strike-abuse-emotet-continue-to-threaten-healthcare-cybersecurity

WHAT IS SEO POISONING?
https://www.crowdstrike.com/cybersecurity-101/attack-types/seo-poisoning/#:~:text=SEO%20poisoning%20is%20a%20technique,closely%20at%20their%20search%20results.

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback