International Journal of Contemporary Research In Multidisciplinary

Review Paper

Deception in the Digital Age: How SEO Poisoning Undermines Online Trust

Ranjan Banerjee[1*] and Ria Roy[2]
[1]Assistant Professor, Computer Science and Engineering, Brainware University, West Bengal, India
[2]Computer Science Engineering, Supreme knowledge foundation group of institution, West Bengal, India

Corresponding Author: *Ranjan Banerjee

DOI: https://doi.org/10.5281/zenodo.11966686

Abstract

To encourage websites to appear in search results in addition to the more conventional methods of spreading malware (such as links or attachments in spam emails), search engine optimization (SEO) techniques have become increasingly popular in recent years due to the rise in malware distribution over the Internet. Attackers are constantly coming up with new and inventive ways to carry out assaults; one such strategy that has gained attention is the choice of search engines for the distribution of malware that has the potential to cause catastrophic outcomes. Though they are relatively new, SEO attacks seem to be common and effective in contaminating the search results for popular queries by disseminating malware. This leads in the creation of several phony pages that target trending keywords once legitimate websites are attacked.

Manuscript Information

- **ISSN No:** 2583-7397
- **Received:** 13-05-2024
- **Accepted:** 14-06-2024
- **Published:** 17-06-2024
- **IJCRM:**3(3); 2024: 106-109

- **Plagiarism Checked:** Yes
- **Peer Review Process:** Yes

How to Cite this Manuscript

Ranjan Banerjee, Ria Roy. Deception in the Digital Age: How SEO Poisoning Undermines Online Trust. International Journal of Contemporary Research in Multidisciplinary.2024; 3(3): 106-109.

KEYWORDS: Poisoning, Search Engine Optimization (SEO), Digital Marketing, Malwares, Websites, Organic Search, Unpaid Search, Search Engine Redirection, Detection.

INTRODUCTION

SEO stands for search engine optimization, which is the application of methods to increase website visibility with the goal of raising a specific URL's ranking in search engine results listings and enhancing the total quantity and quality of unpaid website traffic from organic search engine results. A site's visitor volume can be significantly impacted if it is applied successfully. More than 70% of visitors to most websites find their pages through effective use of search engines [1]. Users now prioritize Search Engine Optimization (SEO) strategies when searching for information online because they can sort through vast amounts of data and choose the most pertinent content. In order to meet this need, digital marketing experts and web developers use a variety of Search Engine Optimization (SEO) techniques that can enhance a website's visibility and promote its ranking in the search results by highlighting its relevance under specific search terms. Website owners always aim to draw in more visitors by optimizing their exposure in relevant search results [1][2].

The search engines use the elements on the pages to assess the pages' relevancy to requests. To stop spammers from attacking, search engines do not publicly reveal the precise criteria that are utilized to assess relevance and ranking. Among the most well-known elements are the text found on the page, the URL, and the title. Given their tendency to condense the information of the

website, the words found in the title and URL are accorded significant weight. Search engines index billions of webpages, and they rank the sites in its index using different variations of page ranking algorithms. The quantity of inbound links determines a page's rank, which indicates the likelihood that a user will click on links at random to reach that page [3].

SEO techniques can be classified into two types:

- **White-Hat SEO techniques:** To improve their website's search engine rating and prepare it for search engine indexing, many businesses may hire marketing consultants. Conversely, in an unethical manner, a variety of methods could be applied to get the same boost. The websites are designed primarily with the end-user in mind, yet they are organized such that search engine crawlers can quickly explore them without any problems. Complying with search engine optimization best practices for quality, white-hat approaches include building a sitemap and using relevant headers and subheadings, among other things.

- **Black-Hat SEO techniques**: These strategies do not adhere to search engine criteria and instead aim to manipulate the ranks. Redirects, hidden text and links, keyword stuffing (crowding the page with unrelated terms), and involvement in link farms are all regarded as black-hat tactics. Search engines disapprove of these tactics, and if one is discovered, a website may be excluded from their index [4].

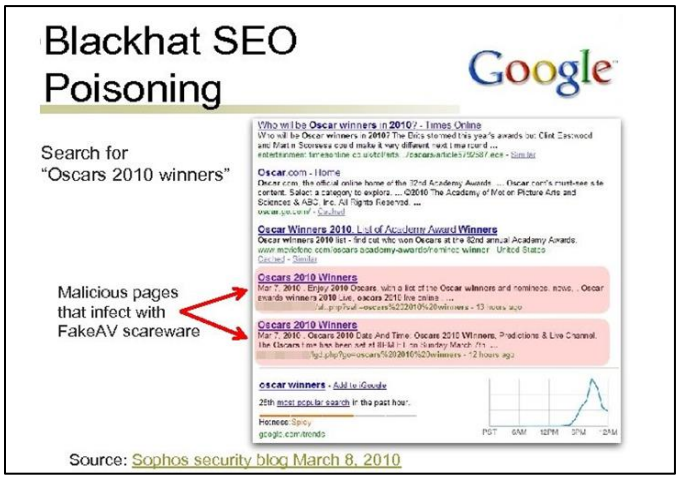


Figure 1: Example of Black-Hat SEO poisoning

In the summarize way, the SEO techniques can be identified according some points below---

White-Hat SEO techniques consist of:

- Good Content
- Proper Titles and Keywords
- Ease of Navigation
- Site Performance
- Quality Inbound Links

Black-Hat SEO techniques consist of:

- Keyword Stuffing
- Cloaking
- Hidden Pages
- Article Spinning
- Duplicate Content

A brief introduction to some of the terms that are discussed while explaining the SEO attacks is enunciated below:

- **Fake antivirus software**: This type of malware deceives users into paying to register a rogue security product by displaying false security alerts.
- **SEO pages:** Often referred to as "SEO poisoned pages," these are intentionally created with a lot of keywords to rank highly in search engine results while rerouting customers to fraudulent websites.
- **SEO kit:** These are the tools for setting up and maintaining an SEO assault website.
- **SEO poisoning:** This term refers to a tactic used to fool search engines into giving an SEO page a high search engine ranking.

Enhanced SEO approaches, on the other hand, are effectively employed to produce favorable economic outcomes that may ultimately raise the website's ranking and boost both the quantity and quality of visitors. Although search engines encourage and even accept legitimate uses of SEO techniques, these techniques are also frequently abused to promote websites among search results and are known as blackhat optimization. On the other hand, dishonest web developers may prefer to abuse these techniques in various ways to obtain (or manipulate) a high ranking within the search results. Deceptive views of a website are produced and given to search engines in blackhat SEO. These views show intelligently generated web pages with inflated relevancy to a selection of selected searchable terms [5][6]. The conversations up to this point have demanded an explanation for a few terms that have become essential to SEO, but they have not revealed who is responsible for the incompleteness of improvement strategies. Following is a list of them:

Traffic Quality: The primary goal is to attract visitors who are really interested in the products that the website has to offer. These visitors are frequently referred to as quality traffic.

Volume of Traffic: The appropriate people navigating from those Search Engine Result Pages (SERPs).

Organic Results: Also known as Unpaid Search, Organic Search refers to any situation in which a searcher can find what they're looking for on the internet without having to pay for it.
In 2007, the first cases of search engine poisoning—which directs users to malicious websites—were documented. Because to its modest investment and authentic appearance, search engine application is appealing to attackers. Malicious pages are hosted on compromised web servers, thereby providing attackers with free resources to use. Users typically have faith in search

engines, and they frequently click on search results without second thought. These malicious pages will be indexed and shown to people in order to produce harmful results, so long as they appear relevant to search engines. Search engine poisoning is a relatively new sort of attack, yet it's already very common and has had a significant impact on major search engines [7].

SEO attacks-An Overview

Attackers using SEO kits, which are PHP scripts packed with trending keywords and phrases, generate web pages targeted at search engines so that they can be indexed by search engines. A link to the SEO page appears highly up in the search engine results when a user searches for keywords; all it takes to expose a user to malware that reroutes them to a malicious website is clicking on the link. After being diverted from the SEO page, there could be several further levels of redirection before the final payload is finally sent.

To illustrate, in the present SEO attacks used to spread malware masquerading as fake antivirus, the victim is usually redirected at least twice before being presented with the malware's fake antivirus webpage, which deceives them into thinking their system is compromised and installing the malware. The selection of keywords is critical to the success of an SEO attack. The shadowy past of search engine optimization is replete with allusions to a practice known as scraping, or splogging, which is the copying of page material with the intention of either promoting linked affiliate sites or sending people to a rogue website in order to earn from advertisements [8][9].

Cloaking Technique

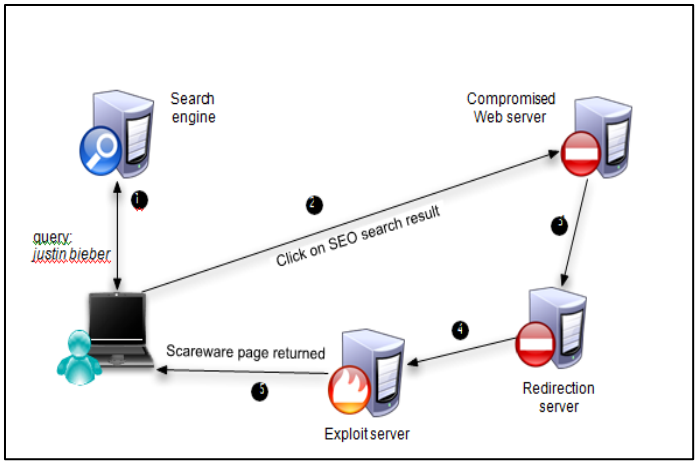
Attackers frequently employ cloaking tactics in situations where the top user receives entirely different material from the internet request based on the communications protocol headers involved. The different opinions are frequently summed up as follows:

Crawler view: The SEO uniform resource locator may reappear on a website response intended to contaminate the software that returns results for the pertinent search query. The uniform resource locator can appear higher in the search results as a result of this.

Browser or user view: Depending on the campaign, the user may be guided through a number of redirects by the SEO universal resource locator before arriving at a final landing page in this scenario.

Referrer view: By relying on the consistent resource locator set contained in the referrer communications protocol header, the SEO can provide the top user with entirely different material in this scenario.

Important conditions found for the effective launch of an SEO poisoning attack are the use of numerous (trendy) keywords and the automatic creation of pertinent content for a large number of pages. Because trendy keywords are popular search items, poisoning the search results of these terms can have a significant impact on a huge number of internet users that use search engines. The creation of fictitious pages and the use of various keywords can help attackers expand the scope of their attacks [10].



Working mechanism and flow of the above-mentioned figure:

The victim types a well-known search query into a search engine (SE), and when they click on one of the results, they happen to be sent to a malicious website that is housed on a compromised server (CS). The request is forwarded to a redirection server (RS) by the hijacked server. After selecting an exploit server, the redirection server points the victim in its direction (ES). The exploit server uses social engineering to try to take advantage of the victim's browser or shows a scareware page.

From the perspective of a genuine user, it is easy to understand how a victim of an SEO keyword poisoning campaign usually becomes unsuspecting of the attack, as the attackers manipulate popular search items to appear with their harmful links in the search results. When a victim searches for such common terms using a search engine, some of the results would lead to servers under the control of attackers. These servers are typically the authentic ones that host SEO pages and have been taken over by the attackers in order to initiate the attack. After making several hops and displaying a scareware page, clicking on the search results takes them to an SEO page that then redirects them to an attack server. For example, the scareware page may entice the user to download and install an application called “anti-virus” that shows a scan for viruses and bright, huge notifications that the victim machine has several infections [11].

Industry Applications

By deceiving search engines and misleading consumers into running the phony antivirus infection, malware propagation through SEO campaigns can be described as astonishing in its simplicity. The victims of the SEO universal resource locator are diverted to entirely different targets. There will be two ways that the pages will function:

- The users are sent to a MaaS (Malware-as-a-Service) platform, which initiates another redirection chain that ends with the final landing page.

- The users go through a sequence of redirects to arrive at the ultimate landing page.

The last landing page websites are from the following top online classes:

- Porn and adult websites
- Websites that provide internet services; in this instance, the SEO campaign's goal is promotion.
- Take use of servers to deliver malware and adware payloads.

CONCLUSION

Using a tactic known as search poisoning, which is essentially an abuse of SEO techniques, the attackers target any search term that can drive more traffic to their malicious websites. This is done by using compromised legitimate websites as a convenient platform for their attacks. By successfully manipulating search engine data, scammers are able to divert gullible people to harmful SEO pages, so starting the attack. The purpose of these assaults is to disseminate malware that poses as an antivirus program. A single point of control and the ability to automatically track the most popular search phrases at any given time are features that some SEO kits offer. The creators and distributors of malware don't really need to alter the recipe as long as the attacks are successful.

REFERENCES

1. Fetterly D, Manasse M, Najork M. Spam, damn spam, and statistics: using statistical analysis to locate spam Web pages. In: Proceedings of the 7th International Workshop on the Web and Databases, WebDB; 2004.
2. Moshchuk A, Bragin T, Gribble SD, Levy HM. A crawler-based study of spyware on the Web. In: Proceedings of the Network and Distributed System Security Symposium, NDSS; 2006.
3. Arthur D, Vassilvitskii S. K-means++: the advantages of careful seeding. In: Proceedings of the 18th Annual ACM-SIAM Symposium on Discrete Algorithms, SODA; 2007.
4. Castillo C, Donato D, Gionis A, Murdock V, Silvestri F. Know your neighbors: Web spam detection using the Web topology. In: Proceedings of the 30th International ACM Conference on Research and Development in Information Retrieval, SIGIR; 2007.
5. Rajab MA, Ballard L, Mavrommatis P, Provos N, Zhao X. The nocebo effect on the web: an analysis of fake anti-virus distribution. In: Proceedings of the 3rd USENIX LEET; 2010.
6. Lu L, Yegneswaran V, Porras P, Lee W. Blade: an attack-agnostic approach for preventing drive-by malware infections. In: Proceedings of the 17th ACM CCS; 2010.
7. Thomas K, Grier C, Ma J, Paxson V, Song D. Design and evaluation of a real-time URL spam filtering service. In: Proceedings of the IEEE S&P; 2011.
8. John J, Yu F, Xie Y, Abadi M, Krishnamurthy A. deSEO: Combating search-result poisoning. In: Proceedings of the 20th USENIX Security; 2011.
9. Google search engine optimization. Available from: http://www.google.com/webmasters/. Accessed June 17, 2024.
10. Kozak. The dirty little secrets of search. Available from: http://www.nytimes.com/2011/02/13/business/13search.html. Published February 2011. Accessed June 17, 2024.
11. How SEO poisoning is used to deploy malware. Available from: https://www.bankinfosecurity.com/how-seo-poisoning-used-to-deploy-malware-a-16882#:~:text=SEO%20poisoning%20is%20an%20illegitimate,websites%20to%20download%20malicious%20files. Accessed June 17, 2024.