**Journal of Neonatal Surgery**
***ISSN(Online): 2226-0439***
***Vol. 14, Issue 13s (2025)***
*https://www.jneonatalsurg.com*

OPEN ACCESS

# Search Engine Poisoning: An Evolving Vector for Malware Distribution via SEO Attacks

**Shankar Prasad Mitra[1], Partha Shankar Nayak[2], Debmalya Mukherjee[3], Shuvrajit Nath[4], Ranjan Banerjee[5]**

[1]Computer Science and Engineering, Brainware University
Email ID: spmitra2016@gmail.com
[2]Computer Science and Engineering-CS & DS, Brainware University
Email ID: psn.cse@brainwareuniversity.ac.in
[3]Computational Sciences Department, Brainware University
Email ID: dbm.cs@brainwareuniversity.ac.in
[4]Computer Science and Engineering-CS & DS, Brainware University
Email ID: shn.cse@brainwareuniversity.ac.in
[5]Computer Science and Engineering, Brainware University
Email ID: rnb.cse@brainwareuniversity.ac.in

Cite this paper as: Shankar Prasad Mitra, Partha Shankar Nayak, Debmalya Mukherjee, Shuvrajit Nath, Ranjan Banerjee, (2025) Search Engine Poisoning: An Evolving Vector for Malware Distribution via SEO Attacks. *Journal of Neonatal Surgery*, 14 (13s), 51-56.

**ABSTRACT**

To promote websites among search results Search engine optimization (SEO) techniques are often used and over the past few years the rising rate of increased spread of malware through the Internet has opened up new dimensions for the attackers along with the traditional techniques for spreading malware (such as through links or attachments in spam emails). The attackers are continuously devising advance methods to launch attacks among which a technique that has came into the limelight is the selection of search engines for distributing malware with high potential to produce devastating results. SEO attacks poisons the search results for popular queries by spreading malware, although recent, appear to be both widespread and effective where legitimate Websites are compromised and a large number of fake pages targeting trendy keywords are generated as a result.

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

## 1. INTRODUCTION

Search Engine Optimization (SEO) can be explained as the techniques employed for improving the website visibility for the purpose of elevating the ranking of a particular URL in the results listings of search engines and improving the overall quality and quantity of the unpaid website traffic through organic search engine results. If implemented successfully, a significant effect upon the volume of traffic hitting a site can be achieved. In case of most websites more than 70% of their visitors reach their pages through the efficient use of Search Engines. The Search Engine Optimization (SEO) techniques are capable of filtering out the most relevant from oceans of information, and have become the first priority of the users while looking for information on the web. In relevant search results the website owners always strive to attract and increase more visitors by optimizing their exposure and in order to fulfill this requirement, digital Marketing professionals and web developers employ a number of Search Engine Optimization (SEO) techniques which can improve the visibility of a website and promote its raking in the search results highlighting its relevance under certain search terms.

The features on the pages are used to determine relevance to queries by the search engines. Search engines do not disclose the exact features officially used to determine the rank and relevance to prevent the spammers from attacking. The words in the title, the URL, and the content of the page are among the most widely known features. The words in the title and in the URL usually summarize the content of the page and as a result they are given high weight. Billions of web pages are indexed and many search engines use variants of the page ranking algorithms for ranking the Web pages in its search index. The rank of a page depends on the number of incoming link and the page rank represents that a user would likely click on links randomly and will end up at that page.

**SEO techniques can be classified into two types:**

- **White-Hat SEO techniques**: Many organisations will recruit marketing consultants to boost the search engine ranking and to optimize their site content for search engine indexing. On the other end of the spectrum in an unscrupulous way, a range of techniques may be used to achieve the same boost. Primarily, the sites are created keeping the end-user in mind, but structured in a way that search engine crawlers can easily navigate the site without encountering any difficulty. Following the quality guidelines recommended by search engines the white-hat techniques are creating a sitemap, having appropriate headings and subheadings, etc.
- **Black-Hat SEO techniques**: These types of techniques try to game the rankings, and do not follow the search engine guidelines. Keyword stuffing (filling the page with lots of irrelevant keywords), hidden text and links, redirects and participating in link farms are considered black-hat techniques. These practices are frowned upon by the search engines, a site could be removed from the search index if caught using such techniques.

The following provides a concise overview of key terminology encountered when examining Search Engine Optimization (SEO) attacks:

- **Deceptive Antivirus Software:** This category of malicious software utilizes fabricated security warnings to deceive users into purchasing counterfeit security solutions.
- **Search Engine Optimized (SEO) Landing Page:** These are web pages engineered to achieve elevated search engine rankings through excessive keyword usage, often redirecting visitors to malicious websites. These are sometimes referred to as SEO-compromised pages.
- **SEO Attack Toolkit:** These are software applications designed to facilitate the creation and administration of websites used in SEO attacks.
- **Search Engine Poisoning:** This refers to the methodology employed to manipulate search engine algorithms, causing malicious SEO landing pages to appear prominently in search results.

Effective Search Engine Optimization (SEO) strategies are valuable tools for driving positive business outcomes, notably enhancing website visibility and attracting a larger, more relevant audience. Search engines endorse ethical SEO practices, but unscrupulous web developers sometimes exploit these techniques for illicit gains, a practice known as black-hat SEO. These individuals manipulate search engine rankings by presenting deceptive versions of their websites to search engine crawlers. These fabricated versions feature meticulously crafted web pages with artificially inflated relevance to targeted keywords.

**To fully grasp the dynamics of SEO, it's essential to define core concepts that underpin optimization practices. These include:**

- **Targeted Traffic:** This refers to attracting visitors genuinely interested in the products or services a website offers. This type of visitor represents high-quality engagement.
- **Volume of Traffic:** This denotes the sheer number of users who click through to a website from Search Engine Results Pages (SERPs).
- **Natural Search Results:** Also known as organic or unpaid search, these results appear in SERPs without requiring payment from the website owner.

The emergence of search engine poisoning, a tactic where malicious actors manipulate search engine results to direct users to malware-laden websites, initially surfaced in 2007. This novel form of cyberattack quickly gained traction due to the inherent appeal of search engines as a vector for malicious activity. The attractiveness stems from the perception of legitimacy that search engines command. Users, accustomed to relying on search results for information and navigation, often approach them with a degree of trust, making them susceptible to manipulation.

A key advantage for attackers lies in the low barrier to entry and minimal investment required. Compromised web servers, often acquired through vulnerabilities or exploits, serve as readily available platforms for hosting malicious pages. These servers effectively become free resources, enabling attackers to disseminate their malware without incurring significant costs. The nature of search engines, designed to index and rank web content based on relevance, inadvertently facilitates this process. If malicious pages are crafted to appear pertinent to specific search queries, they are readily indexed and presented to unsuspecting users.

The inherent trust users place in search engine results is a crucial factor contributing to the efficacy of search engine poisoning. Users, expecting to find relevant and safe links, frequently click on search results without hesitation or suspicion. This implicit trust, while essential for the seamless functioning of search engines, creates a vulnerability that malicious actors exploit.

The mechanics of search engine poisoning involve the creation of seemingly legitimate web pages optimized for specific search terms. These pages, often designed to mimic popular or trending topics, are carefully crafted to deceive both search engine algorithms and human users. Attackers employ various techniques to achieve this, including keyword stuffing, cloaking, and link manipulation.

Keyword stuffing involves the excessive use of relevant keywords within the page content, meta tags, and other elements, aiming to artificially inflate the page's relevance in search engine rankings. Cloaking involves presenting different content to search engine crawlers than to human users, allowing attackers to display optimized content to search engines while redirecting human visitors to malicious websites. Link manipulation techniques, such as creating backlinks from compromised or low-quality websites, are used to artificially boost the page's authority and ranking.

Once a malicious page achieves a high ranking in search results, it becomes a potent tool for distributing malware. Users who click on the link are typically redirected to a website designed to exploit vulnerabilities in their browsers or operating systems, leading to the installation of malware without their knowledge or consent. This malware can range from adware and spyware to ransomware and banking trojans, posing significant risks to users' privacy and security.

The rapid proliferation of search engine poisoning highlights the evolving nature of cyber threats. Despite its relatively recent emergence, this attack vector has become a significant concern for both search engine providers and users. Major search engines have been affected on a large scale, underscoring the challenges in combating this form of attack.

The widespread impact of search engine poisoning necessitates a multi-faceted approach to mitigation. Search engine providers are continuously refining their algorithms to detect and penalize manipulative techniques, such as keyword stuffing and cloaking. They are also investing in advanced security measures to identify and block malicious websites.

User education plays a crucial role in preventing search engine poisoning. Users need to be aware of the risks associated with clicking on search results, particularly those that appear suspicious or irrelevant. They should also be encouraged to employ strong security practices, such as using reputable antivirus software and keeping their browsers and operating systems up to date.

The fight against search engine poisoning is an ongoing battle, requiring constant vigilance and adaptation. As attackers develop new techniques, search engine providers and security professionals must respond with innovative countermeasures. A collaborative effort involving search engine companies, security researchers, and users is essential to effectively combat this evolving threat and protect the integrity of search results.

## 2. A COMPREHENSIVE LOOK AT SEARCH ENGINE OPTIMIZATION (SEO) BASED CYBERATTACKS

SEO-driven cyberattacks represent a sophisticated form of online threat, leveraging the inherent mechanisms of search engine optimization for malicious purposes. At the core of these attacks lies the manipulation of search engine rankings to lure unsuspecting users towards malware-infested websites. Attackers employ specialized tools, often referred to as SEO kits, to automate the creation of web pages designed to rank prominently in search results. These kits, typically composed of PHP scripts, are meticulously crafted to incorporate a dense array of popular keywords and phrases, effectively optimizing the pages for search engine crawlers.

The process unfolds when a user initiates a search query. If the attacker's SEO-optimized page has successfully achieved a high ranking, it will appear prominently in the search engine results. The user, trusting the relevance of the search result, clicks on the link, unwittingly triggering a chain of events that leads to malware exposure. This initial click initiates a redirection process, often involving multiple intermediary steps, before the user is ultimately directed to the malicious website hosting the final payload.

The redirection process is a key component of SEO attacks, designed to obfuscate the true nature of the destination website and evade detection by security measures. In the context of fake antivirus malware distribution, for instance, victims are typically subjected to several layers of redirection before being presented with the counterfeit antivirus webpage. This page is meticulously crafted to mimic legitimate security software, employing scare tactics to convince users that their systems are infected and prompting them to install the malware disguised as a security product.

The selection of keywords is a critical factor in the success of an SEO attack. Attackers meticulously research trending topics, popular search terms, and current events to identify keywords that will attract a large volume of traffic. By targeting these keywords, they increase the likelihood of their malicious pages appearing prominently in search results, maximizing the number of potential victims.

The historical context of SEO reveals a practice known as scraping, which involves the unauthorized copying of content from legitimate websites. This practice, while not directly related to malware distribution, highlights the inherent vulnerabilities within the SEO ecosystem. Scraped content can be used to drive traffic to rogue websites, generating revenue through fraudulent advertising schemes or promoting affiliate links to dubious products.

The exploitation of search engine algorithms for malicious purposes underscores the importance of understanding the

underlying mechanics of SEO. Search engines rely on complex algorithms to determine the relevance and ranking of web pages. These algorithms analyze various factors, including keyword usage, link popularity, and content quality, to provide users with accurate and relevant search results. Attackers exploit these algorithms by manipulating these factors to artificially inflate the ranking of their malicious pages.

The evolution of SEO attacks has necessitated the development of advanced detection and mitigation techniques. Search engine providers are continuously refining their algorithms to identify and penalize manipulative tactics, such as keyword stuffing, cloaking, and link farming. They are also investing in sophisticated security measures to detect and block malicious websites, including those involved in redirection schemes.

User awareness and education are paramount in combating SEO attacks. Users must be cognizant of the risks associated with clicking on search results, particularly those that appear suspicious or irrelevant. They should also be encouraged to employ strong security practices, such as using reputable antivirus software, keeping their browsers and operating systems up to date, and exercising caution when downloading files or installing software from untrusted sources.

The fight against SEO attacks is an ongoing endeavor, requiring a collaborative effort from search engine providers, security researchers, and users. By understanding the tactics employed by attackers and implementing robust security measures, we can mitigate the risks associated with SEO-driven cyber threats and protect the integrity of the online ecosystem.

## 3. CLOAKING TECHNIQUE

Attackers frequently employ cloaking methods to present distinct content to users, based on the protocol headers within the HTTP request. This manipulation results in several distinct views:

- **Search Engine Crawler View:** The SEO URL delivers a response specifically crafted to manipulate search engine indexing, associating it with relevant search terms. This artificially inflates the URL's ranking in search results.
- **User/Browser View:** The SEO URL initiates a series of redirections, ultimately leading the user to a final landing page, the destination of which varies depending on the specific attack campaign.
- **Referer Header View:** The SEO URL serves different content to the user, determined by the URL specified in the HTTP referer header.

Successful SEO poisoning attacks necessitate the strategic use of multiple trending keywords and the automated generation of relevant content across numerous web pages. Targeting popular keywords in search results allows attackers to reach a substantial number of internet users. Furthermore, the creation of fabricated pages targeting diverse keywords broadens the attack's scope.

For a SEO poisoning attack to be launched successfully, important requirements identified are the application of multiple (trendy) keywords as well as generation of relevant content across a large number of pages automatically. Poisoning the search results of trendy keywords can affect a large number of internet users who uses the search engines since the trendy keywords are popular search items. Attackers can effectively increase their attack coverage by generating fake pages and targeting different keywords.


Individuals often become victims of a specific type of online attack when they search for common terms using a search engine. They then select a seemingly relevant result, unaware that it directs them to a website hosted on a server that has been infiltrated by malicious actors. This compromised server acts as a gateway, forwarding the user's request to a redirection server. The redirection server then chooses an exploit server, which the user is subsequently sent to. The exploit server attempts to take advantage of vulnerabilities in the user's web browser or employs social engineering tactics by displaying fear-inducing messages, known as scareware, to trick the user into installing malware.

This attack, known as SEO keyword poisoning, manipulates search engine results by injecting malicious links into popular search queries. In essence, when a user searches for a frequently used phrase, some of the results will lead to servers controlled by the attackers. These servers, often legitimate websites that have been compromised, are repurposed to deliver the attack. Clicking on these manipulated search results initiates a series of redirections, eventually leading the user to an exploit server that presents a scareware page. For example, the scareware page might mimic an antivirus scan, displaying exaggerated warnings of numerous infections and prompting the user to download and install a fake 'security' program.

## 4. APPLICATIONS

The method by which malicious software is distributed through search engine optimization (SEO) attacks is remarkably straightforward: manipulating search engine results and enticing users to execute fraudulent antivirus programs. Victims are often redirected to entirely different destinations than the intended SEO URL. Within these manipulated pages, two primary operational modes can be identified:

- A sequence of redirections that ultimately lead the user to the final landing page.
- Redirection to a Malware-as-a-Service (MaaS) platform, which initiates a subsequent chain of redirections culminating in the final landing page.

The final landing page destinations typically fall into the following major internet categories:

- Websites featuring adult and pornographic content.
- Internet service websites, where the SEO campaign's objective is primarily advertising.
- Exploit servers, which deliver adware or malware payloads.

## 5. CONCLUSION

The digital landscape is increasingly plagued by the insidious practice of search poisoning, a form of Search Engine Optimization (SEO) manipulation employed by cybercriminals to funnel traffic towards their malevolent online domains. This tactic hinges on the exploitation of popular search terms, keywords and phrases known to generate a substantial volume of user inquiries. By strategically targeting these high-traffic areas, attackers maximize their potential reach, ensnaring a wider pool of unsuspecting victims.

A critical component of these attacks involves the utilization of compromised legitimate websites. These websites, often unknowingly, become unwitting hosts for the distribution of malicious content, forming a distributed network that amplifies the attacker's reach. By leveraging the established trust and authority of these compromised sites, cybercriminals enhance the credibility of their fabricated search results, making them appear more legitimate to both search engines and users.

At the heart of search poisoning lies the manipulation of search engine data. Attackers employ various techniques to artificially inflate the ranking of their malicious SEO pages, effectively tricking search engine algorithms into presenting these pages as relevant and trustworthy results. When a user clicks on a manipulated search result, they are redirected to a malicious SEO page, initiating the attack sequence. This redirection process is often seamless, leaving users unaware of the underlying malicious intent.

A prevalent objective of these attacks is the dissemination of counterfeit antivirus malware. These fake security products are designed to deceive users into believing their systems are infected, prompting them to purchase and install the malware under the guise of legitimate security software. This tactic exploits the fear and vulnerability of users concerned about their online safety, leading to significant financial losses and potential system compromises.

The sophistication of modern SEO kits plays a crucial role in the effectiveness of these attacks. These kits often incorporate advanced features, such as real-time tracking of trending search terms, enabling attackers to capitalize on current events and popular topics. Furthermore, they provide centralized control over the attack infrastructure, allowing cybercriminals to manage and monitor their operations with efficiency and precision.

The continued success of search poisoning tactics presents a significant challenge to cybersecurity efforts. The profitability and effectiveness of these methods minimize the incentive for malware developers and distributors to explore alternative strategies. As long as these tactics remain lucrative, cybercriminals are likely to persist in their use, necessitating the development of robust countermeasures.

The implications of search poisoning extend beyond individual users, impacting the overall trust and integrity of online search engines. The erosion of trust in search results can have far-reaching consequences, hindering the flow of information and commerce on the internet.

Combating search poisoning requires a multifaceted approach, involving collaboration between search engine providers, cybersecurity professionals, and users. Search engine providers must continuously refine their algorithms to detect and penalize manipulative techniques, such as keyword stuffing, cloaking, and link farming. They must also invest in advanced

security measures to identify and block malicious websites.

Cybersecurity professionals play a crucial role in developing and implementing tools and techniques to detect and mitigate search poisoning attacks. This includes the development of threat intelligence platforms, intrusion detection systems, and malware analysis tools.

User education is paramount in preventing search poisoning attacks. Users must be aware of the risks associated with clicking on search results, particularly those that appear suspicious or irrelevant. They should be encouraged to employ strong security practices, such as using reputable antivirus software, keeping their browsers and operating systems up to date, and exercising caution when downloading files or installing software from untrusted sources.

The fight against search poisoning is an ongoing battle, requiring constant vigilance and adaptation. As cybercriminals develop new techniques, search engine providers and security professionals must respond with innovative countermeasures. A collaborative effort involving all stakeholders is essential to protect the integrity of the online ecosystem and safeguard users from the insidious threat of search poisoning.

## REFERENCES

[1] D. Fetterly, M. Manasse, and M. Najork. 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] A. Moshchuk, T. Bragin, S. D. Gribble, and H. M. Levy. A crawler-based study of spyware on the Web. In *Proceedings of the Network and Distributed System Security Symposium*, NDSS, 2006.

[3] D. Arthur and S. Vassilvitskii. K-means++: the advan- tages of careful seeding. In *Proceedings of the 18th Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA, 2007.

[4] C. Castillo, D. Donato, A. Gionis, V. Murdock, and F. Sil- vestri. Know your neighbors: Web spam detection using the Web topology. In *Proceedings of the 30th Interna- tional ACM Conference on Research and Development inInformation Retrieval*, SIGIR, 2007.

[5] M. A. Rajab, L. Ballard, P. Mavrommatis, N. Provos, and X. Zhao. The nocebo effect on the web: an analysis of fakeanti-virus distribution. In *Proceedings of the 3rd USENIX LEET*, 2010

[6] L. Lu, V. Yegneswaran, P. Porras, and W. Lee. Blade: an attack-agnostic approach for preventing drive-by malwareinfections. In *Proceedings of the 17th ACM CCS*, 2010

[7] K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song. Design and evaluation of a real- time url spam filtering service. In *InProceedings of the IEEE S&P*, 2011.

[8] J. John, F. Yu, Y. Xie, M. Abadi, and A. Krishnamurthy. deSEO: Combating search-result poisoning. In *Proceedings of the 20th USENIX Security*, 2011.

[9] Google search engine optimization. http://www.google.com/webmasters/.

[10] Kozak The dirty little secrets of search. http://www.nytimes.com/2011/02/13/business/13search.html,February 2011.

[11] https://www.bankinfosecurity.com/how-seo-poisoning-used-to-deploy-malware-a-16882#:~:text=SEO%20poisoning%20is%20an%20illegitimate,websites%20to%20download%20malicious%20files.