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

OPEN ACCESS

The Impact of Evolving Algorithms on Search Engine Optimization Strategies

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

[1]Computational Sciences Department, Brainware University

Email ID: dbm.cs@brainwareuniversity.ac.in

[2]Computer Science and Engineering-CS & DS, Brainware University

Email ID: shn.cse@brainwareuniversity.ac.in

[3]Computer Science and Engineering, Brainware University

Email ID: spmitra2016@gmail.com

[4]Computer Science and Engineering, Brainware University

Email ID: rnb.cse@brainwareuniversity.ac.in

[5]Computer science and engineering-CS & DS, Brainware University

Email ID: psn.cse@brainwareuniversity.ac.in

Cite this paper as: Debmalya Mukherjee, Shuvrajit Nath, Shankar Prasad Mitra, Ranjan Banerjee, Partha Shankar Nayak, (2025) The Impact of Evolving Algorithms on Search Engine Optimization Strategies. *Journal of Neonatal Surgery*, 14 (13s), 46-50.

ABSTRACT

Strategies aimed at improving website visibility in search engine results, known as Search Engine Optimization (SEO), are commonly employed. However, the proliferation of internet-based malware has created new avenues for cybercriminals. In addition to conventional methods like malicious links or attachments in unsolicited emails, attackers are increasingly utilizing sophisticated tactics. A particularly concerning trend is the exploitation of search engines to distribute malware, which can have significant consequences. This approach, termed SEO poisoning, manipulates search results for popular search terms, spreading malware effectively. While a relatively recent phenomenon, it has proven to be both pervasive and impactful, often involving the compromise of legitimate websites and the creation of numerous fake pages targeting trending keywords.

Keywords: *Search ranking enhancement, Website visibility improvement, Online presence optimization, Search result optimization, Web search improvement.*

1. INTRODUCTION

Search Engine Optimization (SEO) encompasses the strategies utilized to enhance a website's visibility within search engine results, ultimately aiming to elevate its ranking for specific URLs. This process drives increased, unpaid website traffic through organic search results. Effective SEO implementation can significantly boost website traffic, with search engines often accounting for over 70% of a site's visitors. SEO techniques serve to sift through vast amounts of online information, enabling users to quickly locate relevant content. Website owners prioritize attracting and expanding their audience by optimizing their online presence. To achieve this, digital marketing experts and web developers employ various SEO tactics that improve a website's visibility and search engine ranking for targeted keywords.

Search engines evaluate website relevance to user queries based on various on-page elements. While the specific algorithms remain undisclosed to prevent manipulation, commonly known factors include title tags, URLs, and page content. These elements, particularly titles and URLs, often summarize the page's content and are therefore weighted heavily. With billions of web pages indexed, search engines employ variations of page ranking algorithms to determine the order of search results. A page's ranking is influenced by the number of incoming links, reflecting the likelihood that a user, browsing randomly, would arrive at that page.

SEO strategies are broadly categorized into two distinct approaches:

Ethical SEO (White-Hat): Many businesses engage marketing professionals to improve their search engine rankings and optimize website content for search engine indexing. Conversely, less scrupulous methods exist to achieve similar results. Ethical SEO focuses on creating websites with the user experience as the primary consideration, while also ensuring search

engine crawlers can easily navigate the site. Adhering to search engine quality guidelines, white-hat techniques include creating sitemaps, using appropriate headings and subheadings, and generating high-quality relevant content.

Unethical SEO (Black-Hat): These techniques attempt to manipulate search engine rankings by disregarding established guidelines. Practices such as keyword stuffing (excessive use of irrelevant keywords), hidden text and links, deceptive redirects, and participating in link schemes are considered black-hat. Search engines strongly disapprove of these methods, and websites found employing them risk being removed from search engine indexes.

Figure 1: Example of Black-Hat SEO poisoning

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

- **Fake anti-virus –** Class of malware with fake security alerts in order to trick them into paying to register the rogue security product.
- **SEO page –** The pages designed to rank highly in search engine results with stuffed keywords yet redirect users to rogue sites sometimes called *SEO poisoned pages*.
- **SEO kit –** These are the application used to create and manage an SEO attack site.
- **SEO poisoning –** A technique used to describe the process of tricking the search engines into ranking an SEO page high up in the search results.

While improved (SEO) techniques square measure with efficiency used for manufacturing positive economical results which might finally improve the ranking of the web site and increase the amount of tourists each in terms of quantity and quality. Legitimate uses of SEO techniques are accepted and even inspired by search engines however they're conjointly usually abused to market internet sites among search results and could be a observe called blackhat Optimization, however dishonest web developers could favor to abuse these techniques in varied ways to achieve (or cheat) a good ranking within the search results. In blackhat SEO deceptive views of an internet site square measure created and bestowed to the search crawlers comprising of showing intelligence crafted web pages with inflated relevancy to a collection of targeted searchable terms. The discussions until currently demands the reason of some terms that became integral components of SEO while not whom truth that means of improvement techniques remains incomplete. They are enumerated below:

- Quality of Traffic: Main aim is to draw in the guests who square measure really fascinated by the merchandise that web site needs to supply which particular traveler are often mentioned below quality traffic.
- Quantity of Traffic: Right folks clicking through from those Search Engine Result Pages (SERPs).
- Organic Results: Organic Search or Unpaid Search is wherever the searcher doesn't need to procure looking their necessities in internet Search Engines.

The first reported instances of Search poisoning luring visitors to malware websites were observed in 2007. To the attackers the application of search engines is attractive reason behind is its legitimate appearance and low investment. On compromised web servers malicious pages are hosted which are effectively free resources for the attackers to utilize. The search engines are generally trusted by the users and they often click on search results without any hesitation or doubt. As long as these malicious pages look relevant to search engines, they will be indexed and presented to end users for obtaining destructive results. Despite being a relatively new form of attack, search engine poisoning is already a huge phenomenon and has affected major search engines on large scale.

SEO attacks-An Overview:

In SEO driven attacks, to create web pages the attackers use SEO kits (PHP scripts typically stuffed with popular keywords and phrases) that will be consumed by search engine crawlers. When a user searches for keywords, a link to the SEO page is presented high up in the search engine results and clicking on the link is all it takes for the user to be exposed to malware which redirects them to some malicious site. There may be multiple additional levels of redirection before the final payload is actually delivered after once redirected from the SEO page.

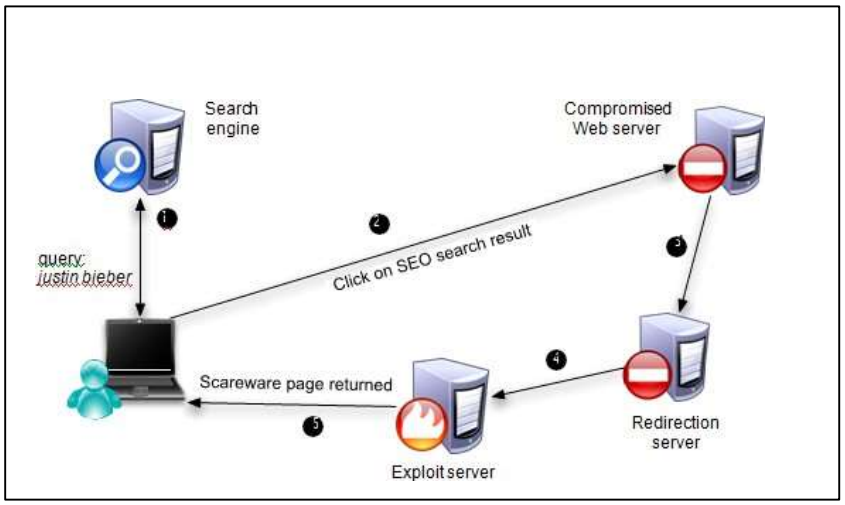
For example, in the current SEO attacks being used to distribute fake anti-virus malware, before being presented with the fake anti-virus web page (which tricks them into believing their system is infected and installing the malware that masquerades as a security product) the victim is typically redirected at least twice. The keywords chosen are very important for a SEO attack to be launched successfully. The murky history of SEO contains abundant references to something known as scraping which involves the copying of page content for the purpose of either driving traffic to a rogue site to profit through ads, or to promote linked affiliate sites.

Cloaking technique:

Cloaking techniques are often used by the attackers wherever the top user is served totally different content depending on the communications protocol headers concerned within the internet request. The various views determined are often summarized below:

- Crawler view: The SEO uniform resource locator can come back on internet response that is targeted towards poisoning the computer program which results for the relevant search term. This may build the uniform resource locator seem higher within the search results.
- Browser or user view: During this case the SEO uniform resource locator can lead the user through a series of redirects before a final landing page, dependent upon the campaign.
- Referer view: Here, the SEO can serve totally different content to the top user, betting on the uniform resource locator set within the referer communications protocol header.

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.



Working mechanism and flow of the above-mentioned figure:

A popular query is issued by the victim to a search engine (SE), and clicks one of the results, which happens to be a malicious page hosted on a compromised server (CS). The compromised server forwards the request to a redirection server (RS). The redirection server picks an exploit server and redirects the victim to it (ES). The exploit server tries to exploit the victim's browser or displays a scareware page to infect the victim through social engineering.

From a legitimate user's point of view, how a victim typically falls prey to an SEO keyword poisoning attack can be understood where the popular search items are poisoned by the attackers so that their malicious links show up in the search results. Some of the results would point to servers controlled by attackers when a search engine is used by the victim to search for such popular terms. These servers are usually the legitimate servers that are used to host SEO pages and have been compromised by the attackers for the purpose of launching the attack. Clicking on the search results leads to an SEO page that redirection to an exploit server after multiple hops that show up a scareware page. For instance, the scareware page might engage the user into downloading and installing an "anti-virus" program depicting an anti-virus scan with large flashy warnings of multiple infections found on the victim system.

Industry Applications

Malware distribution through SEO attacks may simply be represented as stunning in its simplicity by tricking the search engines and engaging users into running the pretending anti-virus malware. The users are redirected to completely different targets victimizing the SEO uniform resource locator. Two modes of operation within the pages will be observed:

- The users undergo a series of redirects to land into the ultimate landing page.
- The users are redirected to a MaaS (Malware-as-a-Service) platform that starts another redirection chain resulting in final landing page.

The final landing page sites belong to the subsequent prime internet classes:

- Adult and porn websites
- Internet services sites; during this case, the SEO campaign's purpose is advertising.
- Exploit servers resulting in adware/malware payloads

2. CONCLUSION

The attackers target any search term that can effectively increase the number of search users to their malicious websites using search poisoning which may be considered as an abuse of SEO techniques by the application of which compromised legitimate websites provide a convenient network of hosts that are being used as a platform for these attacks. The scammers are able to redirect unsuspecting users to malicious SEO pages by successfully poisoning search engine data thus initiating the attack. These attacks are being launched for planned distribution of fake anti-virus malware. Some of the SEO kits provide functionality to automatically track the most popular search terms at any instance of time and also provide a single point of control over. While the attacks continue to succeed, there is little need for the malware authors and distributors to change the formula.

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.