Educational Administration: Theory and Practice
2024, 30(6), 1622-1626
ISSN: 2148-2403
https://kuey.net/

Research Article

Deceptive Ascent: How Attackers Poison Search Results

Ranjan Banerjee[1*], Most Mahabuba Islam[2], Shuvendu Das[3], Debangshu Roy[4], Nikita Dutta[5], Durba Mitra[6], Roni Ghosh[7],

[1*]Assistant Professor Computer Science and Engineering Brainware Universityrnb.cse@brainwareuniversity.ac.in
[2]Department of Computer Science Engineering Brainware University mahabubaislam.ac@gmail.com
[3]Department of Computer Science and Engineering Assistant Professor Brainware University getshuvendu97@gmail.com
[4]Department of Computer Science Engineering Brainware University debangshuroy1010111@gmail.com
[5]Department of Computer Application Regent Education And Research Foundation duttanikita2020@gmail.com
[6]Department of Computer Application Supreme Institute of Management and Technology durba0014@gmail.com
[7]Department of Computer Application Supreme Institute of Management and Technology E-Mail id: mritu5055@gmail.com

Citation: Ranjan Banerjee, et al (2024), Deceptive Ascent: How Attackers Poison Search Results , *Educational Administration: Theory and Practice*, *30*(6), 1622-1626,
Doi: 10.53555/kuey.v30i6.5560

ARTICLE INFO

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

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.

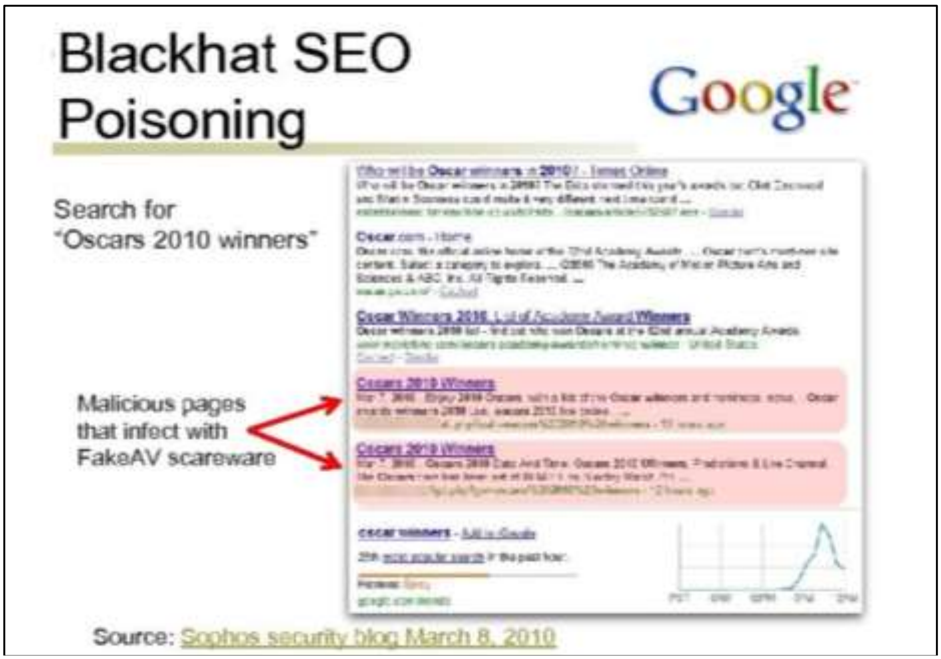
The features on the pages are used to determine relevance to queries by the search engines. Search engines do not disclose the exact features officially used to determine the rank and relevance to prevent the spammers from attacking [3]. The words in the title, the URL, and the content of the page are 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 [1].

Copyright © 2024 by Author/s and Licensed by Kuey. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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[4]. 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 [5]. These practices are frowned upon by the search engines, a site could be removed from the search index if caught using such techniques.



Blackhat SEO Poisoning

Search for "Oscars 2010 winners"

Malicious pages that infect with FakeAV scareware

Source: Sophos security blog March 8, 2010

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 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[6][7]. 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[8]. 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[7][8] . 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 or splogging 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.

- Referrer 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 [9] [10]. 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.

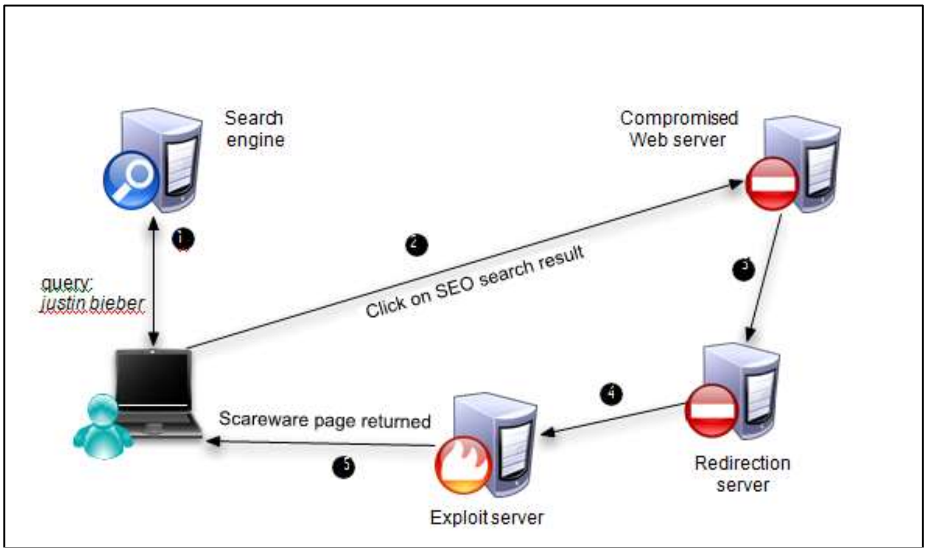
Industry Applications

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 [11]. 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



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. [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. [2] A. Moshchuk, T. Bragin, S. D. Gribble, and H. M. Levy.A crawler-based study of spyware on the Web. In *Pro- ceedings of the Network and Distributed System SecuritySymposium*, NDSS, 2006.
3. [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. [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. [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. [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. [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. [8] J. John, F. Yu, Y. Xie, M. Abadi, and A. Krishnamurthy. deSEO: Combating search-result poisoning. In *Proceedingsof the 20th USENIX Security*, 2011.
9. [9] Google search engine optimization. http://www.google.com/webmasters/.
10. [10]Kozak The dirty little secrets of search. http://www.nytimes.com/2011/02/13/business/13search.html, February 2011.
11. [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.