



| Brief |

Introduction to Social Engineering: Search Engine Optimization Poisoning

B-2024-03-22a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Social Engineering, Phishing, SEO Poisoning

March 22, 2024

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 09:00 AM (EDT) on March 22, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Introduction to Social Engineering: Search Engine Optimization Poisoning

ZeroFox's Social Engineering series breaks down aspects of the threat into digestible reports and outlines defensive actions that can be taken to combat it. Part four of this series takes a deep dive into search engine optimization (SEO) poisoning, why and how threat actors do it, and how the threat can best be mitigated.

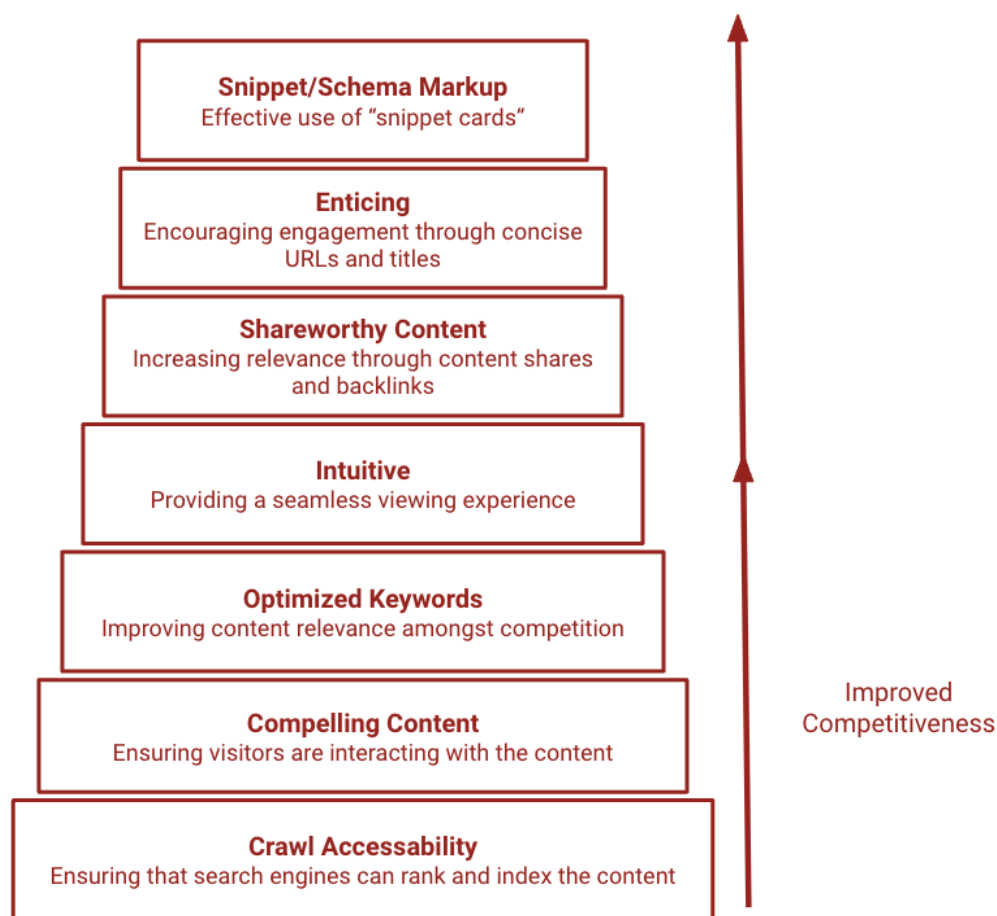
Key Points

- While a legitimate practice, SEO is also used for malicious purposes. This is referred to as SEO poisoning, or “black hat SEO,” and like legitimate SEO, it usually relies upon the premise that users of search engines find the top SERP results the most credible and appropriate to their search, increasing the likelihood they will be visited.
- SEO Poisoning is leveraged by a wide array of threat actors, such as financially-motivated cyber criminals, politically-motivated state actors, ideologically-motivated hacktivists, and organizations seeking a competitive advantage.

- The threat from SEO poisoning to organizations and individuals will almost certainly increase in 2024 as threat actors continually develop new social engineering methods to entice victims and deploy malicious payloads.

| What is Search Engine Optimization

SEO is a series of methods used to increase the visibility of online content and improve its rankings within search engine results pages (SERPs). This is achieved through the optimizing of various elements so as to best satisfy crawling indexing and ranking processes undertaken by search engine algorithms, as well as influence the behavior of users.



"Maslow's" hierarchy of SEO needs

Source: ZeroFox Intelligence

SEO methods can be broken down roughly into three categories:

- Technical: the optimizing of a web page's technical aspects,
- On-site: the optimizing of a web page's content for users and search engines,
- Off-site: the creation of brand-building assets that lead to increased awareness, recognition, and demonstration.

These are broken down into further detail by Maslow's hierarchy of SEO needs, which ranks SEO activities from those used to ensure a web page's "crawlability," to those that help to provide distinction from other top results within SERPs.

Given the increasing dominance of search engines as a means to find online content, understanding how they work in order for them to serve the purposes of an individual or organization has become a key tool in marketing, sales, content creation, and event awareness. The importance of SEO is exemplified by reporting suggesting that a top search result also ranks within the top ten results for up to 1000 separate keywords, and this is almost certain to be exaggerated as top search engine results become increasingly competitive for a growing wealth of digital information.¹

| Search Engine Optimization Poisoning

Individuals and organizations such as marketers, bloggers, media outlets, educational institutions, and government agencies utilize "white hat," legitimate SEO techniques that are widely considered to be ethical, overt, and fall within the acceptable use guidelines of search engine platforms. SEO is also used for malicious purposes, however. This is referred to as SEO poisoning, or "black hat SEO," and like legitimate SEO, it usually relies upon the premise that users of search engines find the top SERP results the most credible and appropriate to their search, increasing the likelihood that they will be visited.

As with other types of social engineering; specific content, images, keywords, and topics are often linked to malicious web pages tailored to attract visitors from specific industries and regions. Visitors of the web page intend to download legitimate software, read a paper, or conduct research.

¹ <https://ahrefs.com/blog/seo-statistics/>

Though the legitimate, intended content can sometimes still be acquired from the web page, various types of malicious activity can take place, seeking to compromise the victim's network. Drive-by downloads can deliver keylogging or stealer malware such as Vidar or SolarMarker to conduct credential theft or downloaders commonly used in SEO poisoning attacks such as BatLoader and Gootloader.

| Threat Actors and Motivations

SEO Poisoning is leveraged by a wide array of threat actors seeking different personal gains. Of these actors, the most notable are the following:

Cyber Criminals: This encompasses a very diverse range of potential threat actors with varying motivations, technical capabilities, and intended payoffs. The vast majority of cyber criminals conducting SEO poisoning are almost certainly financially-motivated and, as such, are ultimately seeking to illicitly gather credentials and other sensitive information such as banking details, deliver malware able to steal information and conduct extortion activities, or generate illicit revenue through traffic redirection. Cyber criminals are very likely to conduct opportunistic attacks, selecting low effort-high payoff targets that are considered likely to facilitate and enable further attacks. It is very likely that certain industries are disproportionately targeted; however, this stems from known IT security practices, associated vulnerabilities, and the existence of contemporary, effective topical lures rather than the innate nature of the industry.

State-Sponsored Actors: Threat actors receiving direction, funding, and support from state entities are very likely able to conduct more complex and technically-demanding attacks than many cyber criminals, which can use SEO poisoning to enhance the chances of success. These actors also seek an array of different ends, including illicit financial gain. The majority of this activity, however, is likely to be ideologically or politically-motivated and used in support of broader information warfare, mis and dis-information campaigns, propaganda dissemination, or the pursuit of strategic influencing goals.

SEO poisoning can also be leveraged in the conducting of cyberespionage campaigns. This would likely encompass techniques, tactics, and procedures (TTPs) often exhibited

by cyber criminals, such as the delivery of information-stealing malware into victim networks, enabled by successful SEO poisoning activity.

Hacktivists: Similar to state-sponsored activists, hacktivists conducting SEO poisoning are not usually financially-motivated, instead seeking to conduct information campaigns. This can be a part of activism, education campaigns, or the spreading of political or event awareness. However, hacktivists may also conduct attacks seeking to cause disruption, leveraging malware and denial-of-service (DoS) attacks—both of which can be facilitated initially through SEO poisoning. The latter of these two motivations is more likely to target organizations or regions specifically, particularly those deemed to be partaking in activities or practices in disagreement with the threat actor.

Competitors: Organizations and businesses engage in SEO poisoning to gain a competitive advantage within the industry or market. This can be achieved by deploying illicit tactics able to increase brand awareness and the reach and readership of their online content, such as web pages, blogs and articles, testimonials, and products.

Organizations also engage in practices that, rather than improve content optimization, seek to sabotage it. This is known as negative SEO, and these practices are often leveraged to promote negative content relating to competing organizations, seeking to damage reputation or undermine credibility. Negative SEO is also conducted against one's own organization in efforts to mitigate reputational damage caused by negative reviews, bad media publicity, or public controversy. This is achieved through the demoting of damaging material and promoting of a counteracting narrative.

| Search Engine Optimization Poisoning Techniques

These threat actors leverage a number of techniques when conducting SEO poisoning, which broadly seeks to exploit either the indexes used by the search engine platform or the algorithms that prioritize results bespoke to the users' search terms. The extent to which these techniques rely upon social engineering varies, though even those primarily focused on manipulating a search engine rely upon active engagement with the malicious content by the victim. Some of the most frequently observed SEO poisoning techniques include:

Keyword stuffing: This is the practice of inserting specific keywords excessively into online content, with the aim of receiving a higher SEO ranking in SERPs. This relies upon the premise that search engine crawling and indexing algorithms will prioritize results with a higher number of matching keywords, associating it with a higher quality match for a user's search terms.² Threat actors using keyword stuffing aim to entice a search engine user to visit a malicious webpage, an event that is more likely to take place if it has a higher ranking.

Keywords are inserted into the main text, captions, headers, and URL of a web page. However, they are also placed in locations more difficult to see upon initial inspection—such as within image metadata, HTML code, anchor texts, references, copyright notices, breadcrumb trails, and in blank spaces within the page using a matching colored background.

Keyword Stuffing Explained

Keyword stuffing is the practice of excessively repeating specific keywords to earn higher rankings within search results. Keyword stuffing can use the content's body text, headings and URL. Keyword stuffing can even use blank space and metadata. Keyword stuffing can result in unnatural paragraphs, harming user experience.

Example of Keyword stuffing

Source: ZeroFox Intelligence

Keyword stuffing is leveraged by threat actors of different motivations. Cyber criminals use malicious web pages to expose the user to malicious hyperlinks and malware, while ideologically-motivated actors seek to expose the user to misleading content. While this technique is still used by threat actors, content featuring keyword stuffing is more likely to be penalized by modern search engine protocols, resulting in a ranking decrease. Today, search engines are more likely to prioritize quality, usability, and comprehensiveness.

² [hXXps://developers.google\[.\]com/search/docs/essentials/spam-policies](https://developers.google.com/search/docs/essentials/spam-policies)

This technique is most likely to be successful when masquerading as a search result with very little information competition, such as those relating to particularly niche subject matter with limited publicly available information. Topical lures are often used to portray authenticity and reduce the victim's suspicions.

SEO Cloaking: This refers to the manipulation of search engine algorithms by revealing different information to that which the search engine user web crawlers are presented with. This is a commonly-used method able to improve the ranking of malicious web pages, and often able to bypass the limitations of keyword stuffing. SEO cloaking can leverage several methods, such as IP cloaking (the differentiation of user IP addresses and those of search engine crawlers) and user-agent cloaking (the use of user-agent information such as browser type and operating system to serve different results to search engines). Javascript cloaking is also used as a method of hiding content from search engine algorithms that will be displayed to users.

Typosquatting: A type of cyber squatting, and also known as URL-hijacking, this is not technically an SEO poisoning method but nonetheless relies upon human error and the creation of malicious web domains. Threat actors conducting this activity use URLs that mimic that of commonly visited websites, only containing errors such as typos, misplaced hyphens or incorrect TLDs. These domains often exploit topical lures, with both the COVID-19 pandemic and the 2020 U.S. Presidential Election reportedly the source of more than 150,000 themed malicious domain names.³⁴

These attacks are more likely to target users who input the intended URL directly into their browser, as search engines are likely to instead display the corrected address. However, malicious web pages that are optimized to search engine algorithms can still be displayed in SERPs.

Typosquatting can also be used in brandjacking attacks, whereby a threat actor seeks to benefit from the trust and familiarity associated with a brand's established reputation for nefarious purposes. Brandjacking can leverage domain spoofing to lure users to a

³ [hXXps://www.splunk\[.\]com/en_us/blog/learn/typosquatting-types-prevention.html](https://www.splunk.com/en_us/blog/learn/typosquatting-types-prevention.html)

⁴ [hXXps://www.sciencedirect\[.\]com/science/article/pii/S0957417422008715](https://www.sciencedirect.com/science/article/pii/S0957417422008715)

malicious web page or URL redirection to direct a user toward the website of a competitor rather than the intended destination.

Negative SEO: This refers to a collection of techniques that aim to degrade the search engine rankings of online content. To achieve this, actors can conduct link spamming and manipulation—the generation of high numbers of low quality backlinks to the target web pages. These links can be generated by automated tools and hosted in link farms or other low-quality web pages. As well as links; negative blogs, comments, and reviews are also spammed across various open-source domains. Content scraping and duplication are other methods whereby a threat actor copies legitimate content from the target web page and distributes it widely across the internet. This can lead to search engines penalizing the targeted web page on the grounds of duplicate content.

These methods of SEO poisoning all rely upon, to different extents, the abuse of Top Level Domains (TLDs) to achieve their intent. As with other methods of social engineering, threat actors prioritize low or no-cost attacks that can lead to a more favorable cost/payoff ratio, and as a result, free, disposable TLDs are a popular tool in the conducting of SEO poisoning. This is because of the short expected shelf-life of domains associated with malicious activity compared to those used for legitimate and legal purposes. Penalization of domains used for phishing and SEO poisoning activity can occur at the hands of law enforcement agencies or TLD authorities. Most often, they lose their utility after being deranked by search engine algorithms.

This has been further exacerbated for threat actors in 2023, with TLD provider Freenom pausing its free registration service for domain extensions such as .tk, .ml, .ga, and .cf.⁵ This was very likely a contributing factor in the reduction in web-facing .ga domains from approximately 5.3 million in May 2023 to 2,600 in August 2023.⁶ This reportedly resulted in a notable decrease in SEO Poisoning attacks emanating from these domains, which, along with other free domains, have traditionally been associated with a significant proportion of incidents.⁷

⁵ [hXXps://securityboulevard\[.\]com/2023/03/sued-by-meta-freenom-halts-domain-registrations/](https://securityboulevard[.]com/2023/03/sued-by-meta-freenom-halts-domain-registrations/)

⁶ [hXXps://www.netcraft\[.\]com/blog/impact-of-freenom-halting-registrations-on-cybercrime/](https://www.netcraft[.]com/blog/impact-of-freenom-halting-registrations-on-cybercrime/)

⁷ [hXXps://www.phishlabs\[.\]com/blog/free-domain-abuse-plummets-in-q1-as-staging-methods-shift/](https://www.phishlabs[.]com/blog/free-domain-abuse-plummets-in-q1-as-staging-methods-shift/)

Resilience – SEO Poisoning

- *Organizations should implement training for employees, focussing on awareness of contemporary threats, phishing vigilance, social engineering resilience, and basic cybersecurity hygiene.*
- *Ensure the relevant personnel are up to date on both proper and malicious SEO techniques using contemporary search engines, enabling more effective and precise incident response.*
- *Organizations should ensure their web pages and other online content are protected by using secure coding practices and updated security plugins and scrutinized with regular website security audits.*
- *Websites should be monitored to prevent irrelevant keywords or hidden data from being inserted.*
- *Review bombing and harmful spam content should be identified and addressed via a comprehensive brand management strategy.*
- *Monitor for signs of SEO poisoning affecting organizational online assets. These include a sudden drop in search engine rankings, an increase in unusual traffic, operating system or web browser security warnings issued to website visitors, and unexpected redirects.*
- *Establish policies and procedures for identifying malicious domains, including identifying and notifying the appropriate authorities and stakeholders.*
- *Engage ZeroFox for services such as ongoing monitoring for impersonated domains, domain takedowns, alerts, and mitigation support.*
- *Organizations should ensure that digital assets that make up technology stacks and attack surfaces are regularly updated as a part of a thorough patch-management process.*

| Outlook

The threat from SEO poisoning to organizations and individuals is almost certain to increase in 2024 as threat actors continually develop new social engineering methods to entice victims and deploy malicious payloads.

Search engine platforms will continue becoming more adept at preventing the undermining of their crawling and indexing algorithms, resulting in greater difficulty for threat actors in leveraging low or no-cost methods such as the abuse of free TLDs. There is a roughly even chance that this will result in a decrease in attacks such as keyword stuffing and some types of cloaking, which typically rely upon the use of multiple, low-investment domains. As threat actors lose access to low-effort approaches, however, they are increasingly likely to exploit those already with consolidated reputations. This will likely lead to an increased emphasis upon web page compromise attacks, malicious redirects, fake landing pages, and pharming attacks.

Optimization techniques are also being increasingly used to promote content on non-search engine platforms, such as video streaming sites and social media platforms. This can provide threat actors the opportunity to conduct poisoning attacks on platforms that will not have the established scrutinization protocol that would be expected from search engines. Threat actors can use promoted content on these platforms to distribute information or malware, a TTP that has been observed taking place via YouTube in the first quarter of 2024.⁸

This diversification, along with increasing difficulty in accessing low-cost TLDs, is likely to encourage threat actors to continually seek new methods of exploiting the trust between individuals and organizations, and various online platforms that use algorithms to display personalized results.

⁸ [hXXps://cybersecuritynews\[.\]com/youtube-videos-deliver-malware/](https://cybersecuritynews[.]com/youtube-videos-deliver-malware/)

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%