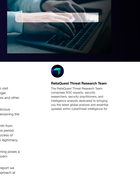
WEBINAR | A Deep Dive into 2023 Cyber Threats | Register Now
Join us on October 19th at 1 PM ET

SEO Poisoning

RELIAQUEST THREAT RESEARCH TEAM | 2 APRIL 2024

EMERGING THREATS | THREAT RESEARCH



Key Points

- Search engine optimization (SEO) poisoning helps cyber-threat actors entice internet users to visit malicious webpages, download malware, and, often, unwittingly provide initial access to a larger victim. This is the first step in a multi-stage attack that can include, ransomware operations and other cybercrimes.
- Threat actors perform SEO poisoning by manipulating search engine algorithms, causing malicious websites to ascend rates of search results. Internet users then click on the links, mistakenly perceiving the sites as legitimate because they have been designed that way.
- In 2023, ReliaQuest observed a 1,000% increase in SEO poisoning malware detections each month from January to June 2023, resulting in an overall 400% increase over the six-month analysis period. Malware as a service toolkits are making SEO poisoning relatively easy, and popular. The success of SEO poisoning campaigns relies on threat actors' exploitation of trending topics, the perception of a site's legitimacy, and certain psychological factors.
- Attacks on the US healthcare and legal sectors are especially common. However, SEO poisoning poses a significant risk to all organizations in businesses of all sizes and sectors. If a malicious payload is delivered, a victim's network and data is at risk.
- Organizations should actively monitor for evidence of SEO poisoning in customer environments. In this report we share indications pulled from our hunts, and targeted recommendations for a proactive approach at defense.

ReliaQuest Threat Research Team
The ReliaQuest Threat Research Team comprises SOC experts, security researchers, and cyber threat intelligence analysts dedicated to bringing the cyber threat analysis and associated updates within cyberthreat intelligence to

Search engines, such as Google and Bing, use SEO techniques to determine which content is most likely to be relevant to a user's search query and rank it accordingly. The goal is to help internet users navigate search engine rank content, and can manipulate search algorithms to boost their own websites' search rankings. This increases their ability to lure unsuspecting users to interact with malicious content.

Interesting the threat is malware as a service (MaaS), such as "Solarmarker" and "Gootloader," which use SEO poisoning to achieve initial access to larger networks. This invites greater compromise that can end in ransomware deployment. Gootloader, for example, is known to be used by ransomware groups. Its deceptive tactic is leading a significant uptick in these attacks. Over the past six months, ReliaQuest observed a 10% increase in SEO poisoning-related malware detections, month over month.

In our experience hunting for indicators of this threat, we've noticed that analyzing a combination of forward and backward looking detections can be helpful. Forward looking detections can help organizations identify the early behaviors a perform that point to a future attack and—ultimately—network intrusion and remediation and subsequent compromise. This report explains SEO poisoning's intricacies, shows its effectiveness in a case study, and offers defense recommendations.

How Does SEO Poisoning Work?

Techniques

SEO poisoning is achieved through various techniques to undermine the integrity of search engine results. The use of link farms and keyword stuffing stand out as the most prevalent we have observed in real-world incidents. Link farms are networks of websites that artificially boost the ranking of a page, while keyword stuffing involves overloading a webpage with irrelevant keywords to boost their own websites' search rankings. This increases their ability to lure unsuspecting users to interact with malicious content.

Link Farms

When ranking content, search engines consider the number of other sites to determine its relevance and authority. Essentially, the more a website is linked to, the higher it appears in a search result. Link farms are networks of websites that exist solely to increase the number of visits. These actors create link farms to trick search engines into perceiving a site as relevant and legitimate.

Keyword Stuffing

Search engines also scan content for keywords. To gauge relevance to a search topic. These actors perform keyword stuffing, which is the practice of filling a site with keywords in an attempt to manipulate the site's content. This technique can be enhanced if the threat actor uses the site to create auto-generated content pages filled with snippets of keywords from other websites. Likely to match a search query. Ultimately, this results in multiple web pages highly ranked for the density of keywords and the likelihood of an exact match.

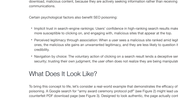


Figure 1: Example of auto-generated content created for keyword stuffing, with underlining indicating these legitimate snippets from respective sources, now aggregated to maximize the chance of matching a given search term (Source: Zscaler)

Attack Chain

SEO poisoning typically involves several stages:

1. Research: A threat actor analyzes search trends to identify popular keywords and topics, such as related to breaking news or seasonal events. This research empowers the threat actor to make their malicious content relevant to a popular subject, and capture the interest of a large audience.

2. Setup: The threat actor builds their malicious content by either hijacking a legitimate site or creating a fake one filled with keyword-rich content and links. In either case, the result is searchable content that seems benign but conceals harmful content.

3. Optimization: The threat actor now uses advanced SEO techniques, such as those described above, to trick search engines and rapidly elevate their site's ranking.

4. Distribution: Once the malicious site achieves a high search ranking, it becomes a trap for users of search engines. The user enters a targeted keyword into the search and sees the malicious site at or near the top of the search results. Trusting the search engine's ranking, the user clicks on the malicious site's link and the trap has been made to card it. On the site, the user will be prompted to download the disguised malware and, potentially, grant initial access to their device.

5. Monetization: The threat actor's ultimate objective is to profit from their activity, and they do this primarily by selling the means to access a compromised user workstation. Access brokers are willing to buy this access, and can resell it to other cybercriminals, including ransomware operators.

Why Is SEO Poisoning So Successful?

SEO poisoning is often more effective than traditional social engineering tactics, the phishing, in aiding initial access to a host. With SEO poisoning, there are more potential victims. Anyone entering the right search terms can fall for the deception, whereas phishing requires a victim to open an email, click on a link, and download, malicious content, because they are actively seeking information rather than receiving unsolicited communications.

Certain psychological factors also benefit SEO poisoning:

- Implicit trust in search engine rankings. Users' confidence in high-ranking search results makes them more susceptible to clicking on, and engaging with, malicious sites that appear at the top.
- Perceived legitimacy through association. When a user sees a malicious site ranked among reputable ones, they may perceive it as genuine or unvetted legitimacy, and they are less likely to question its authenticity.
- Navigation by choice. The voluntary action of clicking on a search result lends a deceptive sense of security. Trusting their own judgment, the user often does not realize they are being manipulated.

What Does It Look Like?

To bring this concept to life, let's consider a real-world example that demonstrates the efficacy of SEO poisoning. A Google search for "army award ceremony protocol pdf" (see Figure 2) might lead users to a counterfeit PDF download page (see Figure 3). Designed to look authentic, the page's content and information mimic official documents. If the visitor interacts with elements of the page, Solarmarker downloads to the user's device.

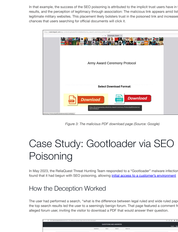


Figure 2: Google results showing malicious PDF download page in second position (Source: Google)

In that example, the success of the SEO poisoning is attributable to the implicit trust users have in top search results, and the perception of legitimacy through association. The malicious link appears amid listings of legitimate military websites. This placement likely bolsters trust in the poisoned link and increases the chances that users searching for official documents will click it.

Figure 3: The malicious PDF download page (Source: Google)

Case Study: Gootloader via SEO Poisoning

In May 2023, the ReliaQuest Threat Hunting Team responded to a "Gootloader" malware infection, and found that it had begun with SEO poisoning, allowing initial access to a customer's environment.

How the Deception Worked

The user had performed a search, "what is the difference between legal sized and wide sized paper?" One of the top search results led the user to a seemingly benign forum. The page featured a comment from an alleged forum user, inviting the visitor to download a PDF that would answer their question.

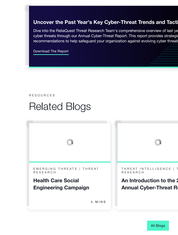


Figure 4: Malicious webpage posing as a forum and containing a PDF download link

The HTML source code of the page revealed the malicious download link. Such simple deceptiveness is the hallmark of SEO poisoning: Having landed on the page, the user was just one click away from downloading a ZIP file that harbored the Gootloader malware.

Figure 5: HTML source code of malicious page

Inside the downloaded ZIP file was a JavaScript-based payload, whose filename corresponded with the user's search query: *what_is_the_difference_between_legal_and_wide_sized_paper_29894.js*. When a victim double-clicked the file, Windows Script Host Services executed it via Windows Script Host (wscript.exe), leading to execution of the first stage malware.

Once executed, the malware established persistence and initiated command-and-control (C2), preparing to deploy a second-stage payload. In this instance, the "Gootkit/SC" remote access trojan (RAT). The RAT would enable attackers to remotely access and extract credentials from the compromised environment.

The initial access the attackers gained to the device eventually led to lateral movement to a server, the deployment of ransomware, and encryption of files. Fortunately, ReliaQuest's managed detection and response (MDR) team identified the malicious files and quarantined them before the network and account access was disabled, removing the attackers' access to the environment.

Hunting for SEO Poisoning

To effectively hunt for malware linked to SEO poisoning in our customers' environments, our approach involves creating two data types:

1. Search engine queries, from forward proxy logs

2. File download event, from endpoint telemetry

We have observed that the name of a downloaded file almost always mirrors the search terms in the user's query. Consequently, this is done to reinforce the user's belief that the downloaded material exactly what they are looking for.

Because the similarity is such a strong indicator, we focus on looking for search terms that correspond with downloaded files' names, particularly files with potentially malicious extensions (e.g., .exe, .zip). For example, if a user searches "Declaration of Independence.zip," and then subsequently downloads a file named declaration-of-independence.zip, we'd—I'll quit now, this is a strong indicator of successful SEO poisoning.

Search Engine Queries

Our methodology begins with gathering forward proxy events with "full URL" data (including the path and parameters of the URL) of traffic to the "search" endpoints for various search engines (e.g., *google.com/search?q=*, *bing.com/search?q=*, *search.yahoo.com/search?p=*, and so on). Then, we treat SERP hosts as not-native search algorithms that would allow us to complete wordless or non-data types.

File Download Data

File downloads are a more difficult data point and can come from multiple sources. The strongest data sources represent a file write explicitly—Sysmon Event ID 11 data from an EDR, for example. For devices without endpoint telemetry, we can look at proxy events with a file extension in the URL path, which is a potential pointer through phone commonly logged proxies create whenever someone clicks on a file's link in the Downloads folder. We then export this data as another component in our offline analysis.

Comparison of Data

Once data has been collected, we employ a Python script to remove duplications, and extract the points of interest. Filenames, search terms, and timestamps for both. We compare the search terms with download filenames, looking for matches. To account for variations in how search terms are represented in a file, the JaccardIndex to score the matches, enabling us to quantify the overlap between the search terms and filenames, a higher score indicates a greater likelihood of SEO poisoning.

We took for instances of at least three words matching between the search terms and filenames. If the match scored above a certain threshold, we record the search terms, filenames, file URL, and the associated hosts score.

For example, the following results of such analysis are shown for a simulated environment with mock data; they show that malware payload file to a seventeen agreement file was downloaded via SEO poisoning after a relevant Bing search.

Search time: 2023-11-16 13:16:41+00:00

Search URL: www.bing[.]com/search?q=Severance+agreement+offer+letter&cvid=51f3fa5cf6c5463a8a5b3f6d08e7758a&ex=1&qs=n

Extracted search terms: *Severance agreement offer letter*

Filename: *Severance_agreement_in_offer_letter_53581.zip*

File time: 2023-11-16 12:57:41+00:00

File URL: www.maliciousdestsite[.]com/rm/Severance_agreement_in_offer_letter_53581.zip

File path: C:\Users\user\Downloads\Severance_agreement_in_offer_letter_53581.zip

Score: 56

Recommendations and Best Practices

SEO poisoning poses an enduring cyber threat, and the US healthcare and legal sectors are frequent targets. Organizations in these industries must remain vigilant and proactive in their defenses, actively observing the continued success of Gootloader. Solarmarker, and other malware spread through SEO poisoning. It has become clear that the real danger lies not just in the initial deception but in the subsequent "downstream" malware infections that can compromise systems.

There are limited options for mitigating SEO poisoning itself. Either the poisoned search result needs to be deprioritized or removed by the search engines, or the domain must be categorized as malicious more quickly (at the proxy/DNS level, or via external threat intelligence). In most cases, SEO poisoning cannot be prevented, but it can be detected. This is why it is critical that organizations monitor for evidence of SEO poisoned. The difficulty of configure makes it almost impossible for SEO poisoning to continue to be used effectively into the mid-term future (three months to one year).

The recommendations below concentrate on enhancing detection capabilities and implementing preventative measures, focusing on the defined malware. These strategies are not only vital for current defense; they also lay the groundwork for adapting to future threats that may emerge as SEO tactics continue to evolve. The following actions are designed to protect our customers from the downstream effects of SEO poisoning, ensuring that their digital environments remain secure.

Enable File Extension Display

By default, Windows hides file extensions from users, which can help prevent non-technically savvy users from accidentally executing malicious files. However, this can also mask dangerous file extensions, such as concealing the nature of malicious files. To mitigate the risk of users unknowingly executing those files, enable the display of file extensions within Windows operating systems.

This helps users identify potentially harmful files masquerading as innocuous ones, such as malware executable Java disguised as a PDF file. Implementing a Group Policy across your organization can ensure that this setting is consistently applied to all users.

Change Default Script Executor to Notepad

Altering the default program that executes script files, specifically JS (JavaScript) and VBS (Visual Basic Script) files, can significantly reduce the risk of script-based malware infections. By default, a user's system. Setting Notepad as the default application for these file types means any attempt to execute the scripts will result in the files being displayed as a text file rather than executed.

This prevents the automatic execution of potentially malicious scripts, offering an additional layer of security. Use a Group Policy to instruct Notepad to open all .vbs and .js files by default.

Implementing these two recommendations can serve as part of a broader defense in-depth strategy, enhancing your organization's resilience against SEO poisoning and other cyberthreats. Always keep your security tools and executing hashing routin.

Uncover the Past Year's Key Cyber-Threat Trends and Tactics
Dive into the ReliaQuest Threat Research Team's comprehensive overview of last year's cyber threats through our Annual Cyber-Threat Report. This report provides strategic recommendations to help safeguard your organization against evolving cyber threats.
Download The Report

RESOURCES

Related Blogs

EMERGING THREATS | THREAT RESEARCH
Health Care Social Engineering Campaign
3 MINS

THREAT INTELLIGENCE | THREAT RESEARCH
An Introduction to the 2024 Annual Cyber-Threat Report
3 MINS

THREAT INTELLIGENCE | THREAT RESEARCH
China-linked Threats to Operational Technology
10 MINS

All Blogs

See GreyMatter in Action

Get a live demo of our security operations platform, GreyMatter, and learn how you can improve visibility, reduce complexity, and manage risk in your organization.

Request A Demo