SUCURI

SEO Spam:
Risks & Mitigation

sucuri.net

SocGholish:
Risks & Mitigation

SEO spam, also known as **spamdexing**, involves the use of deceptive techniques to manipulate search engine rankings. This type of attack is designed to exploit a website's search engine optimization (SEO) to boost the ranking of other sites, often for malicious or unethical purposes. Attackers inject malicious content into a website, which can include hidden text, spammy links, or entire pages designed solely to manipulate search engine algorithms.

SEO spam can occur through various vectors, including:

Vulnerable Plugins:

Attackers exploit outdated or poorly coded plugins to gain access and insert spammy content.

Weak Passwords:

Using brute force attacks to guess login credentials and inject malicious code.

Insecure File Uploads:

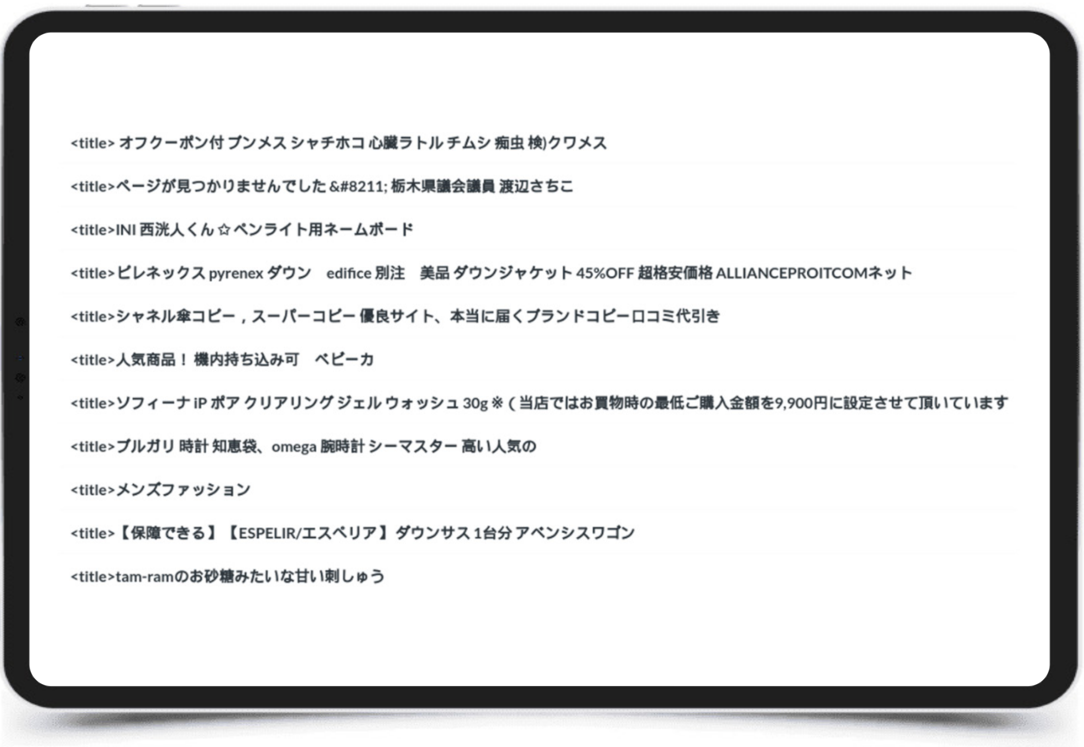
Uploading files containing hidden SEO spam scripts.

SEO Spam Statistics

In 2023, SEO spam was the **third most common malware** found on compromised websites; **20.30%** of all remediated sites were affected by some form of SEO spam.

Our teams eliminated **4,131,724** spam instances from files and cleaned **430,934** spam entries from compromised databases.

Japanese SEO spam was the most prevalent type of spam in 2023, detected and cleaned up from over **10%** of remediated websites — another **157,723** sites were found to be infected with Japanese SEO spam by SiteCheck's remote website scanners.



```
<title> オフクーポン付 プンメス シャチホコ 心臓ラトル チムシ 痴虫 検)クワメス
<title>ページが見つかりませんでした &#8211; 栃木県議会議員 渡辺さちこ
<title>INI 西洸人くん☆ペンライト用ネームボード
<title>ピレネックス pyrenex ダウン　edifice 別注　美品 ダウンジャケット 45%OFF 超格安価格 ALLIANCEPROITCOMネット
<title>シャネル傘コピー，スーパーコピー 優良サイト、本当に届くブランドコピー口コミ代引き
<title>人気商品！ 機内持ち込み可　ベビーカ
<title>ソフィーナ iP ポア クリアリング ジェル ウォッシュ 30g ※（当店ではお買物時の最低ご購入金額を9,900円に設定させて頂いています
<title>ブルガリ 時計 知恵袋、omega 腕時計 シーマスター 高い人気の
<title>メンズファッション
<title>【保障できる】【ESPELIR/エスペリア】ダウンサス 1台分 アベンシスワゴン
<title>tam-ramのお砂糖みたいな甘い刺しゅう
```

Example of Japanese SEO spam page titles found on a hacked website.

How SocGholish Works

SocGholish operates through a series of deceptive and sophisticated tactics designed to trick users and evade detection, including:

Hidden Keywords

Attackers inject keywords into the HTML code of a website in a way that makes them invisible to human visitors but readable by search engines. This can be done using CSS to hide text or placing text in hidden HTML elements.

Cloaking

This technique involves showing different content to search engines and users. For example, the server might detect a search engine bot and serve it optimized content filled with keywords, while regular visitors see normal content.

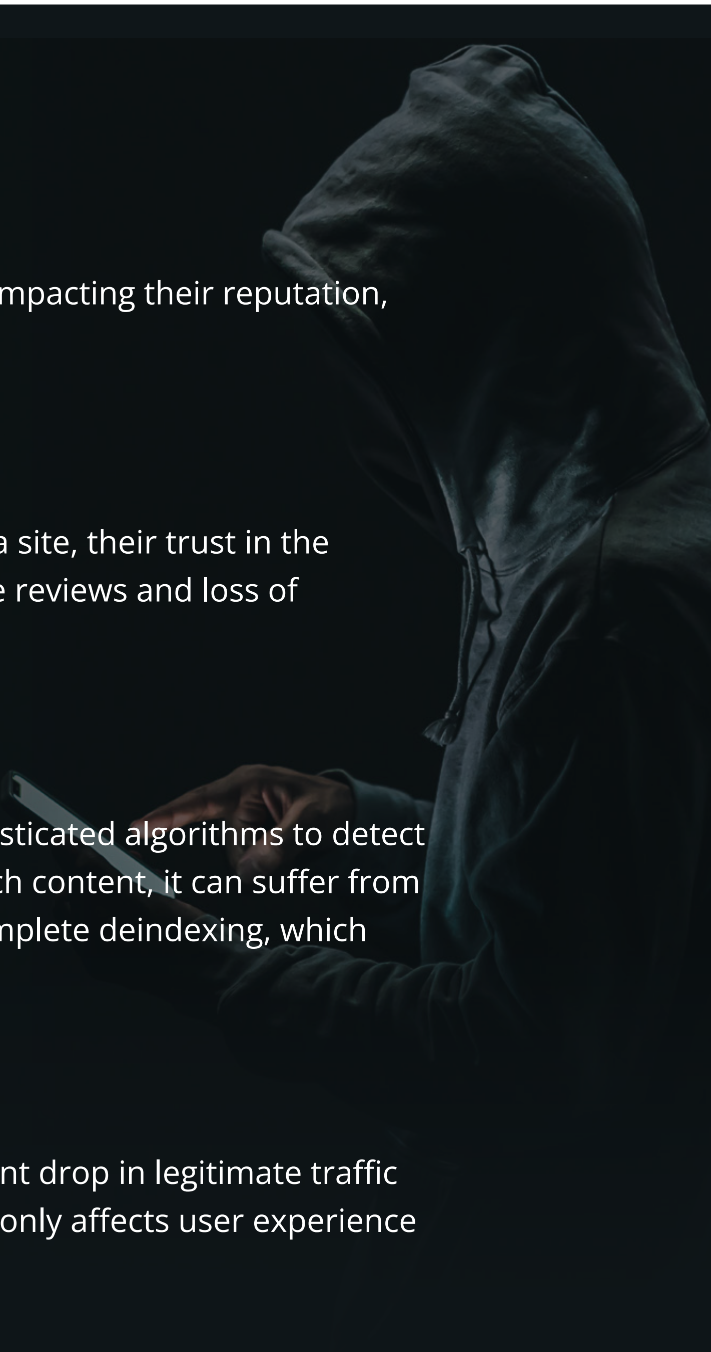
Spammy Links

Inserting links to unrelated or malicious websites, often in the form of comment spam, forum posts, or hidden links in the site's footer or other non-prominent areas.

Redirects

Setting up redirects to send visitors to other sites, often malicious or filled with ads. These redirects can be conditional, only affecting search engine bots or certain types of users.

Risks of SEO Spam



SEO spam poses significant risks to website owners, impacting their reputation, traffic, and overall security:

Damage to Reputation

When users encounter spammy content on a site, their trust in the website diminishes. This can lead to negative reviews and loss of business.

Search Engine Penalties

Major search engines like Google have sophisticated algorithms to detect SEO spam. If a site is found to be hosting such content, it can suffer from penalties ranging from lower rankings to complete deindexing, which severely impacts visibility and organic traffic.

Loss of Traffic

Redirects and cloaking can lead to a significant drop in legitimate traffic as users are diverted to other sites. This not only affects user experience but also

Data Breaches

If attackers gain deep access to a site for SEO spam, they might also have the capability to steal sensitive data, leading to potential data breaches and further compromising the site's integrity.

How Sucuri Helps

Sucuri offers a comprehensive suite of services designed to help website owners mitigate the risks of SEO spam and recover from infections. Here's how Sucuri can assist:

Website Monitoring

Real-Time Insights: By setting up your website on Sucuri's monitoring platform, you receive real-time insights into potential threats and indicators of compromise. This service continuously scans your website for unauthorized changes, suspicious activities, and other anomalies that may indicate an SEO spam attack.

Automated Alerts: Instant alerts are sent out when the system detects any potential issues, enabling rapid response to prevent further damage.

Web Application Firewall (WAF)

Malicious Traffic Filtering: The WAF filters out malicious traffic, blocking attempts to exploit vulnerabilities or inject spammy content into your website. It acts as a barrier between your website and potential attackers.

DDoS Mitigation: While primarily used for preventing spam, the WAF also mitigates Distributed Denial of Service (DDoS) attacks, ensuring your website remains accessible during an attack.

Virtual Patching: The WAF can virtually patch known vulnerabilities in your software, plugins, themes, and other components, providing an additional layer of security without requiring immediate updates.

IP Blocklisting and Allowlisting: You can restrict access to sensitive parts of your website, such as admin or login pages, using IP blocklisting and allowlisting. This helps prevent brute force and ensures only authorized individuals can access critical areas.

Security Features: Implement CAPTCHA and password protection for specific pages to prevent unauthorized access and automated attacks.

Website Backups

Regular Backups: Sucuri offers optional backup services that ensure regular snapshots of your website are taken. These backups can be used to quickly restore your site in the event of an SEO spam infection or other issues.

Secure Storage: Backups are stored securely, protecting your data from potential breaches and ensuring they are readily available when needed.

Advanced Threat Intelligence

Emerging Threat Signatures: Sucuri employs a team of highly skilled malware researchers who constantly create new signatures to block emerging website malware threats, including those related to SEO spam.

Proactive Defense: By staying ahead of the latest threats, Sucuri ensures your website is protected against both known and emerging SEO spam techniques.

Malware Remediation and Cleanup

Experienced Security Analysts: Sucuri's team of security analysts are experienced in identifying and removing SEO spam infections. They perform thorough scans of your website, server, and database to detect and eliminate malicious code.

Comprehensive Malware Cleanup: The cleanup process not only removes the malicious code but also helps to restore your website to its original state, ensuring that any backdoors or vulnerabilities used by attackers are closed.

Post-Infection Support: After the initial cleanup, the Sucuri Platform provides ongoing protection to help prevent future infections and ensure your website remains secure.

Protecting your website from SEO spam and other malicious threats is key to maintaining your online presence and reputation. By leveraging Sucuri's website security platform, you can mitigate the risks associated with SEO spam, quickly recover from infections, and ensure your website remains safe and secure.

For more information or to set up a consultation, please contact us at info@sucuri.net Or Call **1–855-670-2121**

SUCURi

SucuriSecurity | sucuri.net

For more information :

E: sales@sucuri.net
T: 1-855-670-2121