Chapter 8
SEO Poisoning as a Hidden Vector of Cyber Risk and Organizational Compromise

Laura A. Jones
https://orcid.org/0000-0002-0299-370X
Capitol Technology University, USA

ABSTRACT

SEO poisoning has commonly been seen as a consumer cyber risk; recent attacks highlight its threat to enterprise networks. This study examines how SEO poisoning exploits user trust, hybrid work models, and browser synchronization to circumvent traditional firewalls. Real-world incidents demonstrate how attackers manipulate search rankings and leverage browser integrations to deliver malware and steal credentials within work environments. These attack techniques blur the line between external and internal risks, creating hidden dangers typically just outside an organization's main security perimeter that can easily slip through the barrier to evade conventional detection. The research concludes that SEO poisoning is now a critical risk for organizations reliant on SaaS, remote work, and search engines. This study recommends AI-driven detection, enhanced user training, and sector-wide collaboration to counteract these evolving threats and better protect digital trust for cyber professionals, researchers, and policymakers.

DOI: 10.4018/979-8-3373-9918-8.ch008

INTRODUCTION

The digital transformation of the global workforce has fundamentally redrawn the boundaries of organizational cybersecurity. No longer contained within the rigid walls of on-premises data centers, today's enterprise environments are distributed, virtualized, and porous, defined by hybrid workforces, Software-as-a-Service (SaaS) adoption, and the ubiquity of cloud-syncing browser profiles (Somé et al., 2025). Cybercriminals employ AI in contemporary attacks, enabling the creation of highly targeted and scalable attack vectors, such as AI-driven spear-phishing and automated hacking that can breach most modern security measures (Syed, 2022). The Threat Report 2024 found that 67% of workers use personal mobile devices for work-related tasks (Morgan, 2024). This trend has only accelerated since 2020. The modern organizational environment is predominantly digital, with many workers and contractors operating remotely and managing corporate data on personal devices, creating a progressively intricate technological ecosystem that underscores the escalating risk of insider attacks. This profound shift has diluted, and in some cases dissolved, the lines between internal. This challenges the premise that a technical firewall serves as a singular barrier to unauthorized access from external systems. Web application firewalls (WAFs) are employed to identify and prevent attacks on susceptible web applications. These advanced website shields are a prevailing defense against common threats such as hacking, deception, and cross-site scripting (Lasopoulou, 2025); they can protect against a wide range of vulnerabilities (Jadhav, 2023; Kizza, 2024). Although frequently used as a secondary line of defense, WAFs are essential for securing a company's web environment (Nagendran et al., 2020).

In parallel, the cyber threat landscape has evolved with equal dynamism. While much contemporary scholarship examines credential phishing and direct network breaches, an insidious class of attack, search engine optimization (SEO) poisoning, has reemerged with renewed potency (Banerjee & Roy, 2024; Fortinet, 2024; Shaharia, 2025). SEO increases the volume and quality of organic traffic to a website by improving its presence in search engines (Wallenius, 2024); accordingly, attackers use "search poisoning," an abuse of SEO tactics, to target search phrases that drive traffic to their malicious websites. Vectra (2024) defines SEO poisoning as a cyberattack strategy in which adversaries manipulate search engine rankings to prominently feature malicious websites in search results, either to distribute malware or to extract credentials from visitors who mistakenly perceive these sites as legitimate.

Unlike conventional exploits that directly target the corporate perimeter, SEO poisoning manipulates public search engine algorithms (Ganguli, 2024) to place malicious or spoofed websites at the top of organic search results (Banerjee & Roy, 2024; Vectra, 2024). *Search engine optimization (SEO)* is the deliberate process of shaping online content, website architecture, and digital reputation to improve

An Efficient Algorithm for Fast Block Motion Estimation in High Efficiency Video Coding

Murugesan Ezhilarasan, Kumar K. Nirmaland P. Thambidurai (2016). *Emerging Technologies in Intelligent Applications for Image and Video Processing (pp. 132-150).*

www.irma-international.org/chapter/an-efficient-algorithm-for-fast-block-motion-estimation-in-high-efficiency-video-coding/143559