SEO Poisoning Campaign Targets Indian Government and Financial Websites

Vairav Cyber Security News Report

Date: February 18, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

CloudSEK researchers have uncovered a large-scale SEO Poisoning campaign targeting Indian government, educational, and financial websites. The attackers manipulate search engine rankings to redirect users to fraudulent rummy and investment scam sites. Over 200 Indian government domains (.gov.in and .ac.in) have been affected, raising concerns about cyber hygiene and web security across critical sectors.

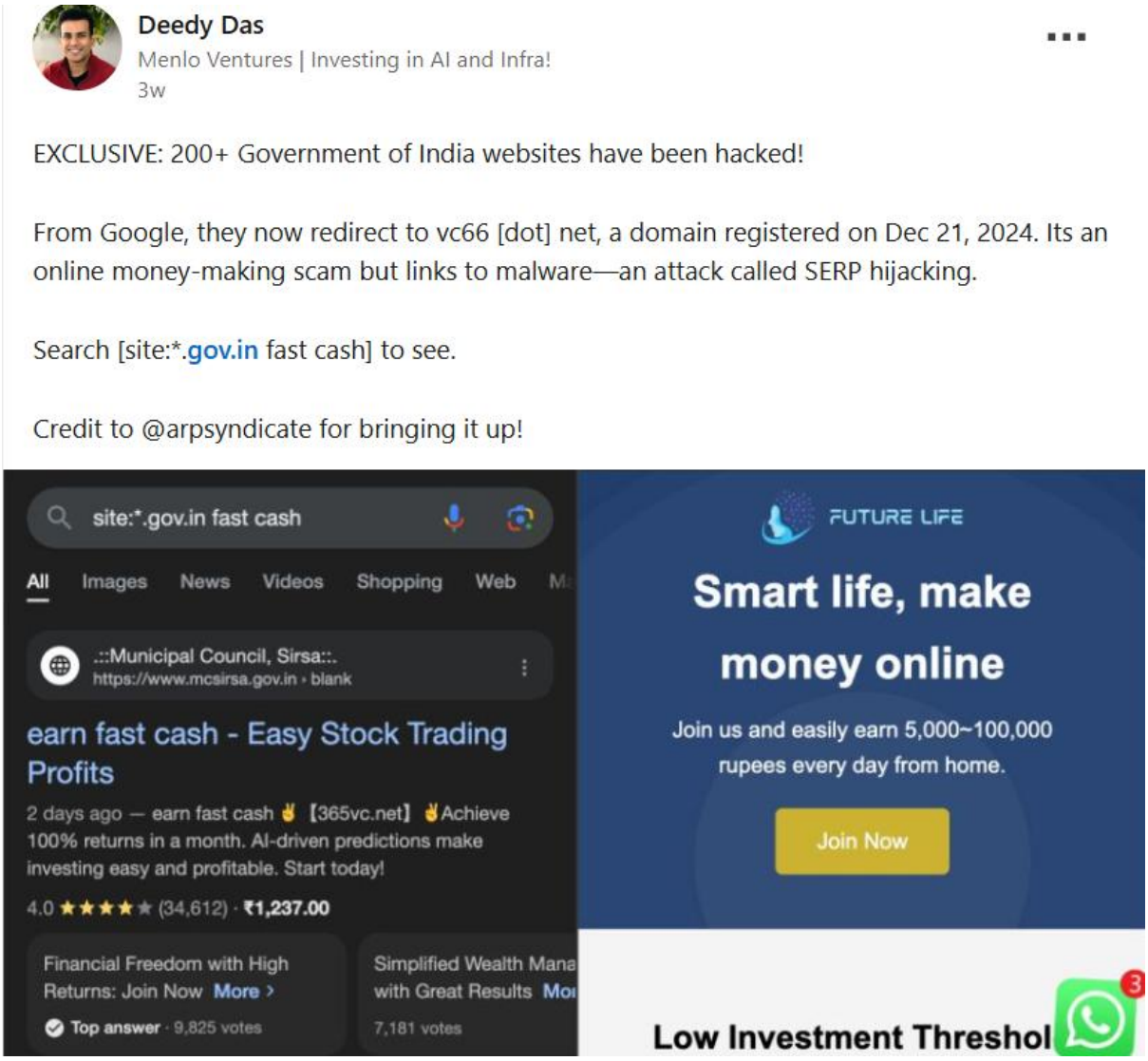

Figure 1: LinkedIn Post

The campaign leverages black-hat SEO techniques, including referrer header manipulation, cloaking, keyword stuffing, backlinking abuse, and CMS exploitation to promote scam websites. Additionally, attackers deploy JavaScript-based redirection mechanisms that differentiate between mobile and desktop users, ensuring a stealthy and effective phishing operation. Beyond India, Malaysia has also reported similar abuses of government

websites, indicating a global threat. Organizations must enhance web security, patch vulnerabilities, and proactively monitor SEO manipulations to mitigate the risks.

DETAILS OF THE INCIDENT

CloudSEK's analysis reveals that cybercriminals have compromised Indian government, educational, and financial websites to conduct SEO Poisoning attacks. The attackers manipulate search engine algorithms to rank scam sites higher, redirecting unsuspecting users to fraudulent rummy and investment websites.

The campaign abuses legitimate government subdomains, misleading users into believing the sites are authentic. Further investigation using Google Developer Tools confirmed the presence of JavaScript-based redirection mechanisms. The attackers use user-agent cloaking to ensure that only mobile users are redirected, while desktop users see a 404 error page, reducing the chances of detection. The exact identity of the attackers remains unknown, but their methods indicate the involvement of cybercriminal networks specializing in SEO fraud and financial scams. The campaign bears similarities to previously identified black-hat SEO operations linked to organized cybercrime groups.

Impact analysis

The SEO Poisoning campaign has led to widespread user redirection to fraudulent gambling and investment scam sites, resulting in significant financial losses for victims. The compromise of government and educational websites has severely impacted their credibility and trustworthiness, raising concerns about cyber hygiene in critical sectors. By manipulating search engine rankings, attackers have distorted search-based research and information retrieval accuracy, making it difficult for users to distinguish between legitimate and malicious content. Additionally, the exploitation of CMS vulnerabilities increases the risk of website defacement and data breaches, potentially exposing sensitive information. The large-scale nature of the attack also poses legal and regulatory challenges, as fraudulent financial schemes continue to thrive through government-linked portals. Furthermore, the campaign's expansion to Malaysia suggests a broader global threat, emphasizing the need for proactive cybersecurity measures to prevent further exploitation.

RECOMMENDED ACTIONS

Technical Mitigations:

- Patch CMS vulnerabilities and update website frameworks regularly to prevent unauthorized script injections.
- Implement security headers (e.g., Content Security Policy, HTTP Referrer Policy) to prevent SEO poisoning and unauthorized redirects.
- Restrict JavaScript execution to trusted sources and prevent unauthorized modifications to website content.
- Blacklist known scam domains and update DNS filtering policies to block fraudulent gambling and investment sites.

Strategic Recommendations:

- Conduct security assessments for government and financial sector websites to identify SEO vulnerabilities.
- Collaborate with search engine providers (Google, Bing) to report abusive ranking manipulations and request blacklisting of malicious sites.
- Strengthen regulatory frameworks to enforce strict cybersecurity compliance for government and financial sector websites.

User Awareness:

- Warn the public about fraudulent search engine results and scam redirection tactics.
- Encourage users to verify website URLs manually before entering sensitive financial details.
- Advise caution against rummy and investment scams, particularly those promising high returns with low risks.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

https://www.hendryadrian.com/the-faux-seo-spiderweb-exploring-how-black-hat-seo-has-riddled-the-indian-internet-space/

https://www.cloudsek.com/blog/the-faux-seo-spiderweb-exploring-how-black-hat-seo-has-riddled-the-indian-internet-space

https://digitalterminal.in/trending/cybercriminals-manipulate-search-rankings-in-india-fueling-black-hat-seo-attacks-across-key-sectors

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com