Advisory on threat actors leveraging SEO poisoning techniques on NIC and government domains.

Vinod Kumar < vinod.vivan@govcontractor.in >

Tue, 20 May 2025 5:50:44 PM +0530

To "A Anbarasu"<pshome@nic.in>,"slaw"<slaw@nic.in>,"divcom"<divcom@nic.in>,"Shri Prashant Goyal"<psud@nic.in>,"chairperson"<chairperson@ndmc.gov.in>,"senv" <senv@nic.in>,"psfin"<psfin@nic.in>,"sgad"<sgad@nic.in>,"pspwd" <pspwd@nic.in>,"pshealth"<pshealth@nic.in>,"commtpt" <commtpt@nic.in>,"adplanningtransport" <adplanningtransport@gmail.com>,"pspower"<pspower@nic.in>,"labcom" <labcom@nic.in>,"Chanchal Yadav, IAS"<ctt.delhi@nic.in>,"ceodelhidjb" <ceodelhi.djb@nic.in>,"cexcise"<cexcise@nic.in>,"wcd"<wcd@nic.in>,"secyart" <secyart@nic.in>,"secyedu"<secyedu@nic.in>,"pstechedu" <pstechedu@nic.in>,"dirtte.delhi"<dirtte.delhi@nic.in>,"SOM DUTT SHARMA" <rcoop@nic.in>,"secservices"<secservices@nic.in>,"chairmandsssb.delhi" <chairmandsssb.delhi@nic.in>,"cdevlop"<cdevlop@nic.in>,"cfss.delhi" <cfss.delhi@nic.in>,"dvigil"<dvigil@nic.in>,"sio-del"<sio-del@nic.in>,"dutcs" <dutcs@nic.in>,"tourismgnctd"<tourism.gnctd@gmail.com>,"commissioner" <commissioner@mcd.nic.in>,"acwmhq"<acwmhq@gmail.com>,"msdpcc" <msdpcc@nic.in>,"director.dlfire"<director.dlfire@nic.in>,"registrar" <registrar@nludelhi.ac.in>,"dirge"<dirge@gov.in>,"dirdcd" <dirdcd@nic.in>,"delhishelter"<delhishelter@gmail.com>,"tourism" <tourism@delhitourism.gov.in>,"cfood"<cfood@nic.in>,"cmd" <cmd@dtc.nic.in>,"mddsiidc"<mddsiidc@gmail.com>,"anjumehta10" <anjumehta10@rediffmail.com>,"ceodpgsenv.delhi" <ceodpgsenv.delhi@nic.in>,"comind"<comind@nic.in>,"ap.delhi"<ap.delhi@nic.in>

Cc "VIVEK PANDEY"<secyit@nic.in>,"VIKAS AHLAWAT"<spl-secyit@delhi.gov.in>,"K. Murugan"<k.murugan@nic.in>,"Pardeep Yadav"<pardeep.kumar43@delhi.gov.in>

Sir/madam,

Please find enclosed "Advisory on threat actors leveraging SEO poisoning techniques on NIC and government domains.

Regards,

1 Attachment(s)

Advisory on threat actors lever...
1.8 MB

Government of NCT of Delhi
Information Technology Department
9th Level, B-Wing, Delhi Secretariat, New Delhi-110002
https://it.delhi.gov.in/

F.17/2/2019-Dir(DeGS)/secy(IT)/CD-93058 /3515-95 Dated 20/05/2025

All ACSs/Pr. Secretaries/Secretaries/HoDs/All Local Bodies/
Boards/Commissions, Govt. of NCT of Delhi

Subject: Advisory on threat actors leveraging SEO Poisoning techniques on NIC and Government Domains.

Madam/Sir,

May kindly refer to the advisory issued by Cyber & Information Security Group (CIS), NIC on subject cited above (copy enclosed).

2. The protection of Government Infrastructure from any Cyber Incident/Attack is a critical area of concern, it is imperative that compliance of above referenced advisory may be ensured and given TOP PRIORITY.

3. In this connection, Departments are requested to direct their respective software development team to ensure that this is strictly complied with.

4. This issues with the approval of Special Secretary (IT).

20/5/25

(K Murugan)
Chief Information Security Officer

Encl: A/a

Copy for information:
1. Secretary to Hon'ble CM, GNCTD
2. Secretary to Hon'ble Minister (IT), GNCTD
3. SO to Chief Secretary, GNCTD.
4. PS to Secretary (IT), GNCTD.
5. Director, DeGS.
6. SIO, NIC, Delhi State Unit.
7. Guard File.

abou

CIS Governance Division
Cyber and Information Security Group,
National Informatics Centre,
A-Block, CGO Complex, Lodhi Road,
New Delhi - 110003 India
csg-advisory@nic.in

NIC-CISG/2025-05/093
Dated: 15-05-2025
Severity: High

Threat actors leveraging SEO poisoning techniques on NIC and Government Domains

Description:

A sophisticated cyber threat campaign is actively targeting NIC and Indian government domains using Search Engine Optimization (SEO) poisoning techniques. Threat actors are manipulating them to redirect users to malicious sites that impersonate legitimate services and lure victims into "pig butchering" scams. In these type of scams, scammers build trust with the victim ("fattening") before financially exploiting them ("butchering") resulting in significant financial losses.

A. Modus Operandi:

- Compromise & SEO Poisoning:
  Attackers exploit vulnerabilities (outdated software, weak credentials) to access government/educational websites, then manipulate content for high search engine rankings on keywords like "Freelance," "Online Business," "Passive Income," "AI & Cloud Computing," and "Gambling."
- Redirection Mechanisms:
  The compromised pages implement a cloaking mechanism that delivers different content based on the user's device, user-agent, and referrer headers. When accessed from a desktop or laptop browser, the page typically returns a 404 error, acting as a decoy to evade analysis. However, when visited from an Android device, the same URL redirects the user to malicious domains such as indo-rummy[.]]vip, which host fraudulent gambling platforms. In contrast, when the page is accessed by search engine crawlers like Googlebot, it promotes fake investment or gambling applications, luring users with promises of passive income or easy profits. This redirection strategy allows the threat actors to avoid detection while maximizing reach to their targeted audience through search engines.

B. **Impact:**

- Financial Losses: Victims are defrauded of significant sums.
- Identity Theft: Personal data may be stolen and misused.
- Brand Damage: Government credibility is undermined.
- Operational Complexity: The campaign is coordinated across multiple domains, making takedown challenging.

C. **Mitigation Measures:**

- Search Engine Reporting: Report the malicious links to search engines like Google and Bing. They can de-index or down-rank the harmful pages.
- Collaboration: Work with the affected website owners to secure their sites by patching vulnerabilities, removing malicious content, and strengthening their security posture.
- Secure File Uploads: Validate file types, restrict file uploads to authenticated users, and use whitelisting for allowed file types.
- Regular Updates and Patching: Keep all software, plugins, and frameworks updated to mitigate known vulnerabilities.
- Use Web Application Firewalls (WAF): Implement a WAF to detect and block malicious file uploads.
- Least Privilege Principle: Configure server permissions to limit file uploads to necessary locations and users.
- Monitor and Audit: Regularly monitor server logs and file system changes to detect unauthorized uploads or modifications.
- Use Security Tools: Deploy tools that can detect and remove web shells, such as antivirus or security plugins specifically designed to find malicious scripts.

D. **Recommendations:**

- Conduct immediate security audits of all NIC and government domains.
- Update and patch all web applications and servers without delay.
- Review user accounts and enforce strong authentication and password policies.
- Make the officials aware about phishing and social engineering risks.
- Report suspicious activity to CERT-In and follow incident response protocols.