Practical Real-time Detection of IPv4 Record Classical Domain Hijacking at Scale

Janos Szurdi
Independent Researcher
Budapest, Hungary
szurdi.janos@gmail.com

Mohammad Ghasemisharif
Palo Alto Networks
Santa Clara, USA
mghasemishar@paloaltonetworks.com

Reethika Ramesh
Palo Alto Networks
Santa Clara, USA
reramesh@paloaltonetworks.com

Zhanhao Chen
Palo Alto Networks
Santa Clara, USA
zhachen@paloaltonetworks.com

Ruian Duan
Palo Alto Networks
Santa Clara, USA
rduan@paloaltonetworks.com

William Melicher
Palo Alto Networks
Santa Clara, USA
bmelicher@paloaltonetworks.com

Daiping Liu
Palo Alto Networks
Santa Clara, USA
dpliu@paloaltonetworks.com

CCS Concepts

• **Security and privacy → Network security**.

ACM Reference Format:
Janos Szurdi, Mohammad Ghasemisharif, Reethika Ramesh, Zhanhao Chen, Ruian Duan, William Melicher, and Daiping Liu. 2026. Practical Real-time Detection of IPv4 Record Classical Domain Hijacking at Scale. In *Proceedings of ACM ASIA Conference on Computer and Communications Security (ASIACCS '26).* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Online Appendix

Likely Domain Hijacking to Fake Ransomware An online training platform *truecoding[.]in* resolved to a Singaporean IP (*184.168.103[.]87*) since 2021. On 16 December 2024, it resolved to *82.180.143[.]236*—an IP located in India. This IP responded with a Ransomware page shown in Figure 2b in the Appendix. Since then we have seen the website recover to the original content (archived link: https://web.archive.org/web/20241224204116/http://www.truecoding.in/) and then again switched back to a different defaced page.

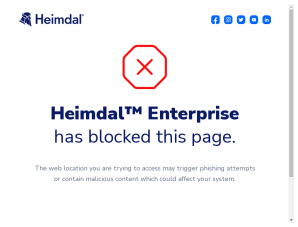
Although we did not see changes in WHOIS registration, the nameserver also changed from *domaincontrol[.]com* to *dns-parking[.]com* and has not recovered. This attack might be a case of different DNS hijacking method as we still see the domain resolve to IP addresses in the same autonomous system as the hijacking IP address. At the same time the current IP addresses are located in different ISPs and countries compared to the hijacking address.

Potential Hijacking of Academic Journal Websites We identified a campaign involving 38 potentially hijacked domains belonging to legitimate academic journals across various fields of study. These domains started to resolve to different IP addresses within the same AS (AS9387). We found this campaign as all 38 domains previously resolved to U.S. IP addresses but post-hijacking resolved to IP addresses in a new AS in the 122.50.0[.]0/24 subnet, geolocated to Pakistan. While the original websites contained meaningful academic content, the hijacked versions displayed only login pages with a title matching the domain name. Interacting with these login pages, we discovered that the submitted usernames and passwords were being sent via a POST request to a backend server hosted at the Pakistani IP address. This behavior suggests a potential credential harvesting operation targeting these journals. None of the 38 domains have recovered.

Other good-to-block detections Figures 1a, 1b, and 1c are screenshots our web crawler got as the result of a DNS response modified by a security vendor to block a domain, a domain seized by law enforcement, and a DNS error, respectively.

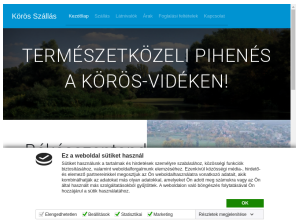
ASIACCS '26, Bangalore, IN

ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn



(a) Domain *cdnn1.img.sputnik[.]az* DNS response modified by security vendor to show block page.

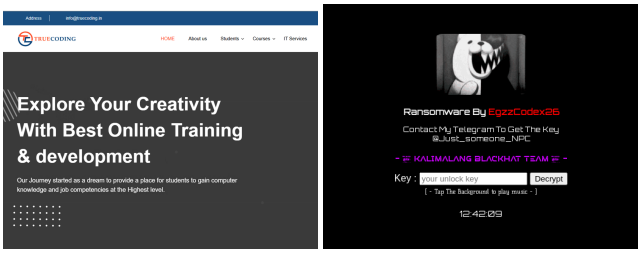
(b) Domain *i27.fastpic[.]ru* seized by law enforcement due to hosting illicit porn.



(c) Domain *z-pao[.]com* pointing to an unrelated benign webpage due to a DNS error.

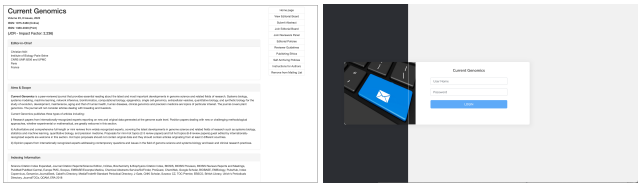
(d) Domain *ftp.conservice[.]com* defaced.

Figure 1: Screenshots of detections and DNS errors.



(a) Before (b) After

Figure 2: *truecoding[.]in* before and after domain hijacking.



(a) Before (b) After

Figure 3: *currentgenomics[.]net* before and after plausible domain hijacking.