Fake CAPTCHA scam targets 2,353 WordPress sites, warns CyberCX

By Shannon Williams

Published: 2025-06-03 · Archived: 2026-04-05 12:42:25 UTC

CyberCX has issued a warning to Australians regarding a phishing campaign targeting WordPress websites through the use of fake CAPTCHA prompts.

The campaign, referred to as DarkEngine, involves threat actors embedding fraudulent CAPTCHA prompts into legitimate WordPress sites, putting website users at risk of various types of malware, including information stealers and remote access tools.

According to CyberCX, at least 2,353 unique websites have been identified as likely compromised by this campaign, with 82 of these belonging to organisations in Australia and New Zealand. Within Australia, the affected websites are predominantly small to medium-sized businesses, spanning a range of sectors from strip clubs to educational platforms for children.

The DarkEngine campaign employs a multi-layered approach. Initially, the perpetrator creates convincing replicas of WP Engine, a management tool widely used by businesses to oversee their WordPress websites. By leveraging a technique known as search engine optimisation (SEO) poisoning, the threat actor is able to position fake WP Engine links above legitimate ones in Google search results. As a result, genuine WP Engine login credentials from website administrators can be harvested and subsequently used to take control of the affected websites to inject fake CAPTCHA prompts.

The campaign's intention is to reach the vast number of visitors to these compromised websites, exposing them to the risk of malware infection through socially engineered prompts.

Katherine Mansted, Executive Director of CyberCX Intelligence, commented on the sophistication of the campaign: "This threat actor is a savvy, highly capable and well-resourced financially-motivated criminal. They are operating a scaled operation here, gaining access to thousands of real websites and infecting them with malware that hits unsuspecting internet users.

"Fake CAPTCHA is an increasingly common technique criminals use to infect Australians' computers with malware. They look similar to real CAPTCHAs – a way to test whether a website visitor is a real person or a bot – but prompt the unsuspecting user to run malicious commands, potentially allowing criminals to gain remote access to their computers.

"Never follow a CAPTCHA command that requires you to copy and paste text and be vigilant for any unexpected downloads after completing a CAPTCHA. Along with unusual URLs, pop-ups and poorly designed CAPTCHA formats, these are the tell-tail signs of a fake CAPTCHA."

The fraudulent CAPTCHA prompts associated with DarkEngine are described as a variation of ClickFix, a social engineering tactic aimed at manipulating users into executing malicious instructions. These techniques have connections to activities used by recognised financially motivated cyber crime groups.

CyberCX Intelligence has stated that it has been reaching out to organisations whose websites have been affected as part of an effort to improve the security of digital communities.

The organisation has provided several recommendations for website administrators and organisations. WP Engine administrators are advised to audit account activity logs for unexpected logins, particularly those originating from unfamiliar proxy services and VPNs. WordPress site administrators should check for any signs of unexpected plugins, content injections within theme files, and successful requests containing keywords such as "emergency_login", "check_plugin", and "urlchange".

Additionally, CyberCX stresses the importance of educating staff about ClickFix techniques, such as fake CAPTCHA, and the risks posed by SEO manipulation potentially leading them to engage with malicious sites. Organisations are also encouraged to consider providing reputable password managers to staff, which can help alert users if the site they are visiting is not legitimate.
