AL2025_29 Malicious WordPress Plugin Disguised as Security Tool Injects Backdoor (June 11, 2025)

Description

A sophisticated malware campaign is targeting WordPress websites using a malicious plugin masquerading as a security tool. Discovered by Wordfence researchers during a routine site cleanup in January 2025, the campaign allows attackers to gain persistent administrative access, execute remote code, and inject JavaScript payloads. The malicious plugin remains invisible in the plugin dashboard, increasing the likelihood of prolonged undetected infections.

Attack Details

The initial infection vector is unclear, though Wordfence speculates the compromise likely occurs through a breached hosting account or stolen FTP credentials. Once the attackers gain access, they modify the wp-cron.php file to automatically install and activate a backdoor plugin initially named WP-antymalwary-bot.php.

The plugin performs a self-check and enables an emergency login function, which uses the emergency_login GET parameter to grant administrator access. If the correct cleartext password is provided, the script retrieves admin accounts from the database and logs the attacker in.

Further, the malware registers an unauthenticated REST API endpoint that allows:

- Insertion of arbitrary PHP code into active theme header.php files
- Clearing of plugin caches
- Execution of additional malicious commands via POST requests

Later variants of the malware can also inject base64-decoded JavaScript into the site's <head> section a tactic typically used for ad injection, spam delivery, or malicious redirections. Alarmingly, if the plugin is deleted, the modified wp-cron.php file recreates and reactivates it upon the next visit to the site.

The Command and Control (C2) infrastructure for this malware has been traced to a server in Cyprus. Some elements of the code and behavior suggest a possible connection to a 2024 supply chain attack.

Remediation

Immediate Actions:

- Back up your current site and database.
- Temporarily take the site offline to prevent further compromise.
- Manually inspect and clean wp-cron.php, header.php, and the plugin directories.
- Remove any plugins with suspicious names listed in the IoCs.

Check for Administrator Hijack:

- Review administrator accounts and login history.
- Change all admin account passwords.
- Look for unauthorized REST API routes or functions in theme files.

Enhance Security:

- Reset all FTP, hosting, and database credentials.
- Reinstall core WordPress files from a clean source.
- Install a reputable security plugin (e.g., Wordfence, Sucuri) and perform a full site scan.

Post-Cleanup Monitoring:

- Monitor access logs for suspicious GET/POST parameters.
- Enable file change detection.
- Set up alerts for unauthorized plugin activations or changes.

Report and Inform:

- Report the incident to your hosting provider.
- Notify any impacted users if sensitive data was exposed.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- The Hacker News. (n.d.). Fake security plugin on WordPress enables remote admin access for attackers. Retrieved from The Hacker News. https://thehackernews.com/2025/05/fake-security-plugin-on-wordpress.html
- Toulas, B. (2025, April 30). WordPress plugin disguised as a security tool injects backdoor. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/wordpress-plugin-disguised-as-a-security-tool-injects-backdoor/