مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Malicious WordPress Plugin Masquerading as Anti-Malware Tool

Tracking #:432317156

Date:02-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that the Wordfence Team has identified a sophisticated malware strain that disguises itself as a legitimate WordPress plugin.

TECHNICAL DETAILS:

The Wordfence Team has identified a sophisticated malware strain that disguises itself as a legitimate WordPress plugin named WP-antymalwary-bot.php. Initially discovered on January 22, 2025, this malware operates with multiple advanced functionalities: remote code execution via the REST API, unauthorized administrative access, and persistent reinfection via wp-cron.php. Its obfuscation techniques and ability to reestablish itself even after removal pose a severe threat to WordPress site integrity. Wordfence has since released both malware signatures and firewall rules for detection and mitigation.

Technical Details

Infection Characteristics:

- **Filename:** WP-antymalwary-bot.php (also seen as addons.php, scr.php, wp-performance-booster.php)
- **Persistence Mechanism:** Alters wp-cron.php to reinstall the malicious plugin if deleted.
- **Obfuscation:** Hides itself from the WordPress plugin dashboard.
- **Initial Entry Point:** Likely through compromised hosting or stolen FTP credentials.

Malicious Capabilities:

1. **Administrator Hijack:**
   - emergency_login parameter in a GET request gives attackers admin access.
   - Selects the first admin user and logs in using a hardcoded password.
2. **Remote Code Execution (RCE):**
   - REST API endpoint allows unauthenticated execution of PHP code.
   - Supports commands like cache clearing and code injection into header.php.
3. **Malvertising and JavaScript Injection:**
   - Pulls base64-encoded JavaScript ad URLs from compromised servers.
   - Injects malicious script tags into HTML <head> sections of themes.
4. **C&C Communication:**
   - Pings Command & Control server at http[:]//45.61.136.85:5555 every minute with site info.
   - Uses scheduled cron jobs (wp_schedule_event) to automate pinging.
5. **Auto-Reinstallation:**
   - wp-cron.php ensures reactivation by writing and executing the plugin on each visit if removed.

Indicators of Compromise (IOCs)

Indicator	Type
WP-antymalwary-bot.php	Malicious file
emergency_login	Malicious GET param
check_plugin	Alive check param
45.61.136.85	Command & Control IP
Modified wp-cron.php	Persistence mechanism
Malicious JavaScript in header.php	Code injection

RECOMMENDATIONS:

- Scan all WordPress installations for the presence of suspicious plugins, especially files named WP-antymalwary-bot.php.
- Audit and review the contents of wp-cron.php for unauthorized modifications.
- Remove any detected malicious plugins and restore clean versions of core files, themes, and plugins from trusted backups.
- Change all administrative credentials and enforce strong password policies

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.wordfence.com/blog/2025/04/interesting-wordpress-malware-disguised-as-legitimate-anti-malware-plugin/