Backdoor Di Balik Plugin Keamanan Wordpress

Categories : WordPress

X-WP-SPAM-SHIELD-PRO Backdoor Hacker Di Balik Plugin Keamanan WordPress

Seorang penjahat cyber telah menyembunyikan kode untuk backdoor PHP di dalam kode sumber plugin WordPress yang menyamar sebagai alat keamanan bernama "X-WP-SPAM-SHIELD-PRO."

Penyerang itu jelas berusaha memanfaatkan reputasi plugin WordPress yang sah dan sangat populer yang disebut "WP-SpamShield Anti-Spam," alat anti-spam populer untuk situs WordPress yang di-host sendiri.

Sebagai gantinya, pengguna yang mendownload X-WP-SPAM-SHIELD-PRO mendapat kejutan buruk berupa backdoor yang memungkinkan penyerang membuat akun admin miliknya sendiri di situs tersebut, mengunggah file di server korban, menonaktifkan semua plugin, dan lebih.

Plugin yang berfokus pada keamanan menghasilkan backdoor yang

merugikan

Semua perilaku jahat itu tersebar di file plugin palsu. Sebagai contoh:

- **class-social-facebook.php** – berpose sebagai alat perlindungan spam media sosial, namun kode yang ditemukan dalam mengirimkan daftar daftar plugin pengguna ke penyerang dan secara opsional menonaktifkan semua plugin. Alasan untuk menonaktifkan semua plugin adalah mematikan semua plugin yang berfokus pada keamanan lainnya yang memblokir akses ke fungsi masuk atau mendeteksi login tidak sah dari hacker.
- **class-term-metabox-formatter.php** – mengirim versi WordPress pengguna ke penyerang.
- **class-admin-user-profile.php** – mengirimkan daftar semua pengguna admin WordPress ke penyerang.
- **plugin-header.php** – menambahkan user admin tambahan bernama mw01main.
- **wp-spam-shield-pro.php** – ping server hacker yang terletak di mainwall.org, membiarkan penyerang mengetahui kapan pengguna baru memasang plugin palsu tersebut. Data yang dikirim file ini mencakup pengguna, kata sandi, URL situs yang terinfeksi, dan alamat IP server.

Baca Juga : Daftar Ping WordPress Untuk Pengindeksan Lebih Cepat

File yang terakhir ini juga menyertakan kode untuk memungkinkan penyerang mengunggah arsip ZIP di situs korban, unzip, dan kemudian jalankan file di dalamnya.

Pada saat para periset keamanan menemukan plugin jahat tersebut, file ZIP yang ditawarkan untuk diunduh telah rusak, namun para ahli percaya bahwa penyerang tersebut menerapkan versi tercemar dari plugin WordPress All In One SEO Pack yang terkenal.

Hati-hati dengan apa yang Anda pasang di situs WP Anda

Menurut Sucuri, perusahaan keamanan cyber yang menemukan X-WP-SPAM-SHIELD-PRO, plugin tersebut tidak pernah berhasil masuk ke repositori WordPress Plugins resmi, tersedia melalui sumber lain.

Secara keseluruhan, plugin ini membuat pengguna khawatir dengan keamanan situs mereka, namun kenyataannya, ini adalah kejatuhan mereka.

Baca Juga : Daftar Ping WordPress Untuk Pengindeksan Lebih Cepat

Sama seperti dengan Google Play Store, Apple App Store, dan toko resmi lainnya, pengguna WordPress disarankan untuk memasang plugin gratis dari repositori plugin resmi saja. Sementara repositori Plugin WordPress dan adminnya jauh dari sempurna, plugin yang ditawarkan untuk diunduh biasanya dipatroli oleh masyarakat, yang sering mendeteksi dan melaporkan sebagian besar ancaman ini pada waktunya.

Related Posts

- Tema WordPress Terbaik Optimasi Google AdSense 2017
- Daftar Ping WordPress Untuk Pengindeksan Lebih Cepat

Related Post

Perbedaan Image Releases dengan Image Licenses

views 27

Cara Mendapatkan Backlink Edu dan Gov di Disqus

views 103

Sisi Lain Internet Marketing

views 27

10 Tips Pemasaran di Sosial Media

views 24