Attacco ai siti WordPress sfrutta uno zero-day in un plugin

Mar 22, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, News, RSS, Vulnerabilità 0

Due gruppi di pirati informatici hanno preso di mira Easy WP SMTP. Il bug nel popolare plugin consentiva di prendere il controllo totale del sito.

WordPress è di gran lunga il più popolare backend per la gestione di siti Internet. Stando ai dati di **W3Techs**, è usato per il **33,4% dei siti nel mondo**. Il Content Management System, però, ha anche un altro primato, decisamente meno entusiasmante: **il 90% dei siti hackerati nel corso del 2018 utilizzavano il CMS open source**.

La colpa sarebbe dei numerosi plugin disponibili per la piattaforma, i cui frequenti bug di sicurezza rappresentano una manna per i pirati informatici che puntano a compromettere i siti Web.

A confermare la teoria degli esperti di sicurezza arriva il caso di **Easy WP SMTP**, un plugin per WordPress che consente di configurare e gestire il servizio SMTP per l'invio delle email con più di **300.000 installazioni attive**.

Gli attacchi ai siti che utilizzano Easy WP SMTP sono stati rilevati per la prima volta venerdì scorso da **NinTechNet**, che ha pubblicato un alert sul suo sito Internet.

I cyber-criminali sfruttavano una vulnerabilità nella **versione 1.3.9 del plugin** relativa al sistema di importazione ed

esportazione delle impostazioni, che in pratica consente le operazioni anche senza autenticazione.

Peggio ancora: il sistema di importazione consente di modificare la **wp_options table**, permettendo ai cyber-criminali di creare un nuovo utente con poteri di amministratore e **prendere il controllo del sito Internet**.

Gli attacchi, esaminati nel dettaglio anche dagli esperti di **WordFence** in questo report, sarebbero stati portati da due distinti gruppi di pirati informatici, che hanno utilizzato esattamente la tecnica individuata da NinTechNet nei primi attacchi.

I due gruppi, però, utilizzerebbero la falla di Easy WP SMTP per scopi diversi. Uno, infatti, si limiterebbe a inserire una backdoor che gli consente l'accesso. Il secondo, invece, utilizzerebbe i siti per **dirottare i visitatori su pagine Web contenenti malware**.

Il suggerimento, per tutti gli amministratori WordPress che utilizzano il plugin, è naturalmente quello di aggiornare immediatamente alla **nuova versione 1.3.9.1** ed eseguire una scansione e controllo del proprio sito per verificare che non sia già stato colpito.

Please follow and like us:

Attacco mirato all’Arabia Saudita. Gli esperti: “i pirati cercavano soldi”

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/03/22/attacco-ai-siti-wordpress-sfrutta-uno-zero-day-in-un-plugin/