Raffica di attacchi a WordPress sfruttano due bug in Social Warfare

Apr 24, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Intrusione, Malware, News, RSS, Vulnerabilità 0

Le falle di sicurezza nel popolare plugin permettono di prendere il controllo del Content Management System. A rischio più di 40.000 siti Internet.

Si chiama **Social Warfare** ed è un plugin piuttosto popolare tra gli utenti **WordPress**. La sua funzione è quella di consentire la condivisione di contenuti sui social media.

Lo scorso 21 marzo, però, sono emerse due vulnerabilità (CVE-2019-9978) che affliggono le versioni di Social Warfare precedenti alla 3.5.3.

La **Unit 42** di **Palo Alto Networks**, che ha individuato le falle di sicurezza, spiega nel suo report che l'uso combinato dei due bug (uno è un classico Cross Site Scripting, l'altro un'esecuzione di codice in remoto) permette nella pratica di eseguire codice PHP sul sito e, di conseguenza, prenderne il completo controllo.

A distanza di un mese, sempre secondo i ricercatori della Unit 42, la situazione è tutt'altro che risolta. Nonostante la disponibilità di un aggiornamento che corregge i bug, infatti, sono ancora tantissimi i siti Internet gestiti con WordPress che utilizzano una versione vulnerabile del plugin.

Nel frattempo, i cyber-criminali stanno sfruttando la situazione in ogni modo e nei bassifondi del Web si

moltiplicano gli exploit che sfruttano le falle di sicurezza.

Gli attacchi individuati dai ricercatori puntano a prendere il possesso dei siti per poi sfruttarli per i loro scopi. I payload utilizzati variano **dall'iniezione di JavaScript per la generazione di cripto-valute** (sullo stile di CoinHive) al **dirottamento del traffico verso pagine Web con inserzioni pubblicitarie o exploit che installano malware sui computer dei visitatori**.

E il fenomeno non accenna a decrescere: una ricerca su Internet, sempre riportata nello studio della Unit 42, indica che ci sono attualmente più di **42.000 siti che utilizzano il plugin** e molti di questi hanno ancora una versione non aggiornata.

Un problema, quello dei plugin WordPress vulnerabili ad attacchi, che nel mondo della sicurezza è ben conosciuto ma per il quale si stenta ancora a trovare soluzioni efficaci. Secondo una ricerca di **Imperva**, infatti, il 98% delle vulnerabilità di WordPress del 2018 sono collegate a un plugin.

Please follow and like us:

Database senza protezione: esposte le password di 2 milioni di reti Wi-Fi

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/04/24/raffica-di-attacchi-a-wordpress-sfruttano-due-bug-in-social-warfare/