Attacchi a 900.000 siti WordPress

Mag 06, 2020 Marco Schiaffino Attacchi, In evidenza, News, RSS, Vulnerabilità 0

I pirati sfruttano principalmente vulnerabilità XSS per inoculare una backdoor nel codice dei siti Internet presi di mira.

Ancora **WordPress**, ancora una campagna di attacchi a tutto campo che cercano di garantire ai pirati informatici un accesso ai siti Internet per prenderne il controllo e inserire al loro interno dei collegamenti a pagine nocive.

La segnalazione arriva da Defiant, che ha rilevato un'insolita attività online che sta prendendo di mira alcune vulnerabilità di plugin per WordPress.

In questo caso, spiegano i ricercatori, i pirati informatici non si stanno muovendo sulla base di nuove falle di sicurezza, ma sembrano puntare più che altro sulla legge dei grandi numeri. **I cyber criminali, infatti, starebbero utilizzando una serie di vulnerabilità piuttosto datate, nella speranza di individuare siti Internet i cui amministratori non hanno eseguito gli aggiornamenti che le correggono**.

Una strategia che, purtroppo, rischia di dare i suoi frutti. Molti utenti WordPress, infatti, hanno un atteggiamento piuttosto "lassista" negli aggiornamenti e nemmeno le ultime novità introdotte dagli sviluppatori del **Content Management System** (che prevede l'aggiornamento automatico dei plugin) sembra poter arginare questo tipo di attacchi.

Nel dettaglio, i cyber criminali starebbero sfruttando cinque vulnerabilità relative ad alcuni plugin e più precisamente **Easy2Map**; **Blog Designer**; **WP GDPR Compliance**; **Total Donations** e nel tema **Newspaper**.

La maggior parte delle vulnerabilità sono semplici XSS (Cross Site Scripting) e la maggior parte delgi attacchi sono quelli che sfruttano la falla in Easy2Map, corretta nell'agosto del 2019.

L'attacco sfrutta due modalità. Nel caso in cui l'amministratore non abbia effettuato l'accesso, lo script usato dai pirati imposta un dirottamento del sito verso un indirizzo malevolo. Se invece l'amministratore ha eseguito l'accesso, cerca di iniettare una backdoor nel file PHP.

La soluzione, concludono i ricercatori, è piuttosto semplice: aggiornare i plugin in questione.

Condividi l'articolo

Attacchi hacker a un aereo? Qualcosa si può fare

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/05/06/attacchi-a-900-000-siti-wordpress/?utm_source=rss&utm_medium=rss&utm_campaign=attacchi-a-900-000-siti-wordpress