WP-VCD: ecco come i pirati fanno strage di siti WordPress

Nov 05, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 1

Gli attacchi vanno avanti da almeno due anni e sfruttano plugin e temi "taroccati" al cui interno si nasconde il codice malevolo.

Una gang di pirati informatici sta infettando migliaia di siti Internet basati su WordPress per utilizzarli come trampolino di lancio per distribuire pubblicità indesiderate e pop-up che conducono a pagine contenenti malware.

Si chiamano **WP-VCD** e sono stati individuati dagli esperti di sicurezza di **WordFence**. Come riportano in un articolo i colleghi di **ZDNet**, che hanno ricevuto in esclusiva il report, il gruppo di cyber-criminali è attivo almeno dal febbraio 2017 e ha infettato un numero impressionante di siti Web.

Piuttosto che utilizzare vulnerabilità del popolare **Content Management System (CMS)**, WP-VCD usa come vettore di attacco temi e plugin piratati che distribuisce attraverso una serie di siti Internet specializzati.

www.download-freethemes.download
www.downloadfreethemes.co
www.downloadfreethemes.space
www.downloadnulled.pw
www.downloadnulled.top
www.freenulled.top
www.nulledzip.download

www.themesfreedownload.net
www.themesfreedownload.top
www.vestathemes.com

I siti in questione, spiegano i ricercatori, possono contare su un SEO strepitoso e di conseguenza compaiono in cima alla lista dei risultati sui motori di ricerca quando vengono usate parole chiave relative a temi piratati (nulled) per WordPress.

A dare una mano ai pirati informatici è anche il sistema usato da Google per classificare i risultati delle ricerche. Com'è noto, infatti, l'algoritmo di **Google** considera principalmente i collegamenti esterni e WP-VCD ha quindi gioco facile a "pompare" il SEO di questi siti, semplicemente inserendo i collegamenti nei siti Internet che compromettono.

Insomma: una sorta di circolo vizioso (o di loop) che gli consente di rendere sempre più efficaci i loro strumenti di attacco man mano che mietono nuove vittime.

Il malware che i pirati informatici utilizzano per prendere il controllo dei siti su cui vengono installati i temi infetti è

decisamente “rognoso”. Come prima cosa crea una backdoor creando un utente (100010010) con privilegi di amministratore.

In secondo luogo, inserisce una copia di sé stesso in tutti i temi caricati sul CMS. La logica è cristallina: nel caso in cui il legittimo amministratore del sito decida di cambiare tema (magari perché ha soltanto provato quello scaricato) il malware rimarrà attivo.

Condividi l’articolo

Italia quarta al mondo per attacchi basati su Macro Microsoft lavora per rendere più sicuro il suo ecosistema

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/11/05/wp-vcd-ecco-come-i-pirati-fanno-strage-di-siti-wordpress/