Una nueva campaña maliciosa comprometió más de 15,000 sitios web de WordPress en un intento de redirigir a los visitantes a portales de preguntas y respuestas falsos.

> *«Estos redireccionamientos maliciosos parecen estar diseñador para aumentar la autoridad de los sitios del atacante para los motores de búsqueda»,* dijo el investigador de Sucuri, Ben Martin en un informe publicado la semana pasada, calificándolo de *«truco inteligente de SEO de sombrero fresco»*.

La técnica de envenenamiento del motor de búsqueda está diseñada para promover un *«puñado de sitios falsos de preguntas y respuestas de baja calidad»*, que comparten plantillas de creación de sitios web similares y son operados por el mismo atacante.

Un aspecto notable de la campaña es la capacidad de los hackers para modificar más de 100 archivos por sitio web en promedio, un enfoque que contrasta drásticamente con otros ataques de este tipo en lo que solo se manipula una cantidad limitada de archivos para reducir la huella y escapar de la detección.

Algunas de las páginas más comúnmente infectadas incluyen *wp-signup.php, wp-cron.php, wp-links-opml.php, wp-settings.php, wp-comments-post.php, wp-mail.php, xmlrpc.php, wp-activate.php, wp-trackback.php y wp-blog-header.php.*

Este extenso compromiso permite que el malware ejecute los redireccionamientos a los sitios web elegidos por el atacante. Cabe mencionar que las redirecciones no ocurren si la cookie wordpress_logged_in está presente o si la página actual es wp-login-php (es decir, la página de inicio de sesión) para evitar levantar sospechas.

El objetivo final de la campaña es *«dirigir más tráfico a sus sitios falsos y aumentar la autoridad de los sitios mediante clics de resultados de búsqueda falsos para que Google los*

clasifique mejor y obtengan más tráfico de búsqueda orgánico real».

El código inyecto logra esto al iniciar una redirección a una imagen PNG alojada en un dominio llamado *«ois[.]is»* que, en lugar de cargar una imagen, lleva al visitante del sitio web a un URL de resultado de búsqueda de Google de un dominio de preguntas y respuestas de spam.

No está claro de inmediato cómo se violan los sitios web de WordPress, y Sucuri dijo que no notó que se explotaran fallas obvias en los complementos para llevar a cabo la campaña.

Se sospecha que se trata de un caso de fuerza bruta en las cuentas de administrador de WordPress, por lo que es esencial que los usuarios habiliten la autenticación de dos factores y se aseguren de que todo el software esté actualizado.