Los hackers están aprovechando un plugin de WordPress legítimo pero desactualizado para utilizar sitios web como backdoor en una campaña en curso, según reveló Sucuri.

El complemento en cuestión es Eval PHP, lanzado por un desarrollador llamado flashpixx. Permite a los usuarios insertar páginas de código PHP y publicaciones de sitios de WordPress que después de ejecutan cada vez que se abren las publicaciones en un navegador web.

Aunque Eval PHP nunca recibió una actualización en 11 años, las estadísticas recopiladas por WordPress muestran que está instalado en más de 8000 sitios web, y la cantidad de descargas se disparó de una o dos en promedio desde septiembre de 2022 a 6988 el 30 de marzo de 2023.

Solo el 23 de abril de 2023, se descargó 2140 veces. El complemento ha acumulado 23,110 descargas en los últimos siete días.

Sucuri, propiedad de GoDaddy, dijo que observó que a las bases de datos de algunos sitios web infectados se les inyectaba código malicioso en la tabla «wp_posts», que almacena las publicaciones, páginas y la información del menú de navegación de un sitio. Las solicitudes se originan en tres direcciones IP distintas con sede en Rusia.

> *«Este código es bastante simple: usa la función file_input_contents para crear un script PHP en el docroot del sitio web con la puerta trasera de ejecución remota de código especificada»,* dijo el investigador de seguridad Ben Martin.

> *«Aunque la inyección en cuestión deja caer una backdoor convencional en la estructura del archivo, la combinación de un complemento legítimo y un cuentagotas de backdoor en una publicación de WordPress les permite volver a infectar fácilmente el sitio web y permanecer oculto. Todo lo que el atacante debe hacer es visitar una de las publicaciones o páginas infectadas y la puerta trasera se inyectará en la estructura del archivo».*

Sucuri dijo que detectó más de 6000 instancias de esta puerta trasera en sitios web comprometidos en los últimos seis meses, y describió el patrón de insertar el malware directamente en la base de datos como un *«desarrollo nuevo e interesante».*

La cadena de ataque implica la instalación del complemento Eval PHP en sitios web comprometidos y su uso indebido para establecer backdoors persistentes en múltiples publicaciones que a veces también se guardan como borradores.

«La forma en que funciona el plugin Eval PHP es suficiente para guardar una página como borrador para ejecutar el código PHP dentro de los códigos cortos [evalphp]», explicó Martin, y agregó que las páginas no autorizadas se crean con un administrador del sitio real como autor, lo que sugiere que los hackers pudieron iniciar sesión exitosamente como un usuario privilegiado.

Una vez más, el desarrollo señala cómo los hackers están experimentando con diferentes métodos para mantener su punto de apoyo en entornos comprometidos y evadir los escaneos del lado del servidor y el monitoreo de la integridad de los archivos.

Se recomienda a los propietarios de sitios web que aseguren el panel de administración de WP y que estén atentos a cualquier inicio de sesión para evitar que los hackers obtengan acceso de administrador e instalen el complemento.