Los perpetradores de amenazas están llevando a cabo ataques de fuerza bruta contra sitios de WordPress mediante la explotación de inyecciones maliciosas de JavaScript, según revelan recientes descubrimientos de Sucuri.

Estos ataques, que adoptan la forma de ataques de fuerza bruta distribuidos, se centran en *«objetivos de sitios web de WordPress desde los navegadores de visitantes completamente inocentes y desprevenidos»*, según explicó el investigador de seguridad Denis Sinegubko.

Esta actividad forma parte de una ola de ataques previamente documentada en la que sitios de WordPress comprometidos se utilizaron para insertar criptoextractores como Angel Drainer directamente o redirigir a los visitantes del sitio hacia sitios de phishing de Web3 que contenían malware extractor.

La última versión es notable porque las inyecciones, encontradas en más de 700 sitios hasta la fecha, no cargan un extractor, sino que utilizan una lista de contraseñas comunes y filtradas para realizar ataques de fuerza bruta contra otros sitios de WordPress.

El ataque se despliega en cinco etapas, permitiendo al perpetrador aprovechar sitios ya comprometidos para lanzar ataques de fuerza bruta distribuidos contra otros posibles sitios víctimas:

1. Adquisición de una lista de sitios de WordPress objetivo.
2. Extracción de nombres de usuario reales de los autores que publican en esos dominios.
3. Inyección del código JavaScript malicioso en sitios de WordPress ya infectados.
4. Lanzamiento de un ataque de fuerza bruta distribuido en los sitios objetivo a través del navegador cuando los visitantes llegan a los sitios comprometidos.
5. Obtención de acceso no autorizado a los sitios objetivo.

> Sinegubko explicó: *«Por cada contraseña en la lista, el navegador del visitante envía la solicitud de la API XML-RPC wp.uploadFile para cargar un archivo con*

> *credenciales cifradas que se utilizaron para autenticar esta solicitud específica. Si la autenticación tiene éxito, se crea un pequeño archivo de texto con credenciales válidas en el directorio de cargas de WordPress».*

Actualmente se desconoce qué llevó a los perpetradores a cambiar de criptoextractores a ataques de fuerza bruta distribuidos, aunque se cree que el cambio pudo haber sido impulsado por motivos de lucro, ya que los sitios de WordPress comprometidos podrían monetizarse de diversas maneras.

Sin embargo, los extractores de billeteras criptográficas han causado pérdidas de cientos de millones de activos digitales en 2023, según datos de Scam Sniffer. El proveedor de soluciones antifraude Web3 ha revelado que los extractores están aprovechando el proceso de normalización en el procedimiento de codificación EIP-712 de la billetera para eludir las alertas de seguridad.

Este desarrollo se produce después de que el informe DFIR revelara que los perpetradores están explotando una vulnerabilidad crítica en un plugin de WordPress llamado 3DPrint Lite (CVE-2021-4436, puntuación CVSS: 9.8) para implementar la cáscara web Godzilla con el fin de obtener acceso remoto persistente.

También sigue a una nueva campaña SocGholish (también conocida como FakeUpdates) dirigida a sitios de WordPress, en la que el malware de JavaScript se distribuye mediante versiones modificadas de plugins legítimos que se instalan aprovechando credenciales de administrador comprometidas.

> El investigador de seguridad Ben Martin señaló: «*Aunque ha habido diversas modificaciones maliciosas de plugins y varias campañas diferentes de actualizaciones falsas de navegadores, el objetivo, por supuesto, siempre es el mismo: engañar a los visitantes desprevenidos del sitio web para que descarguen troyanos de acceso remoto que luego se utilizarán como punto de entrada inicial para un ataque de ransomware».*