Se estima que más de un millón de sitios web de WordPress fueron infectados por una campaña en curso para implementar malware llamado Balada Injector desde el año 2017.

La campaña masiva, según Sucuri de GoDaddy, *«aprovecha todas las vulnerabilidades de plugins y temas conocidas y descubiertas recientemente»* para violar los sitios de WordPress. Se sabe que los atacantes se desarrollan en oleadas una vez cada pocas semanas.

> *«Esta campaña se identifica fácilmente por su preferencia por la ofuscación de String.fromCharCode, el uso de nombres de dominio recién registrados que alojan scripts maliciosos en subdominios aleatorios y por los redireccionamientos a varios sitios fraudulentos»,* dijo el investigador de seguridad Denis Sinegubko.

Los sitios web incluyen soporte técnico falso, premios de lotería fraudulentos y páginas de CAPTCHA maliciosas que instan a los usuarios a activar las notificaciones *«Permita verificar que no es un robot»,* lo que permite a los hackers enviar anuncios de spam.

El informe se basa en hallazgos recientes de Doctor Web, que detalla una familia de malware de Linux que explota vulnerabilidades en más de dos docenas de complementos y temas para comprometer los sitios web vulnerables de WordPress.

En los años intermedios, Balada Injector se ha basado en más de 100 dominios y una plétora de métodos para aprovechas vulnerabilidades conocidas (por ejemplo, inyección de HTML y URL del sitio), y los atacantes intentan principalmente obtener las credenciales de la base de datos en el archivo php wp-config.

Además, los ataques están diseñados para leer o descargar archivos de sitios arbitrarios, incluyendo copias de seguridad, volcados de bases de datos, archivos de registro y errores, así como para buscar herramientas como adminer y phpmyadmin que los administradores del sitio podrían haber olvidado al completar las tareas de mantenimiento.

En última instancia, el malware permite la generación de usuarios administradores de WordPress falsos, recopila datos almacenados en los hosts subyacentes y deja puertas traseras para un acceso persistente.

Balada Injector realiza además búsquedas amplias en directorios de alto nivel asociados con el sistema de archivos del sitio web comprometido para ubicar directorios grabables que pertenecen a otros sitios.

> *«Por lo general, estos sitios pertenecen al webmaster del sitio comprometido y todos comparten la misma cuenta de servidor y los mismos permisos de archivo. De esta forma, comprometer solo un sitio puede potencialmente otorgar acceso a varios otros sitios 'gratis'»,* dijo Sinegubko.

En caso de que estas vías de ataque no estén disponibles, la contraseña de administrador se fuerza brutalmente usando un conjunto de 74 credenciales predefinidas. Por lo tanto, se recomienda a los usuarios de WordPress que mantengan actualizado el software de su sitio web, eliminen los complementos y temas no usados y utilicen contraseñas de administración de WordPress seguras.

Los hallazgos se producen semanas después de que Unit42 de Palo Alto Networks descubriera una campaña de inyección de JavaScript maliciosa similar que redirige a los visitantes del sitio a páginas fraudulentas y de adware. Más de 51,000 sitios web se han visto afectados desde 2022.

La actividad, que también emplea String.fromCharCode como técnica de ofuscación, lleva a las víctimas a páginas con trampas explosivas que las engañan para que habiliten las notificaciones automáticas haciéndose pasar por una verificación de CAPTCHA falsa para mostrar contenido engañoso.

> *«El código JS malicioso inyectado se incluyó en la página de inicio de más de la mitad de los sitios web detectados. Una táctica común usada por los operadores de la campaña fue inyectar código JS malicioso en los nombres de archivo JS de uso frecuente (por ejemplo, jQuery) que probablemente se incluyan en las páginas de inicio de los sitios web comprometidos»*, dijeron los investigadores de Unit42.

> *«Esto ayuda potencialmente a los atacantes a atacar a los usuarios legítimos del sitio web, ya que es más probable que visiten la página de inicio del sitio web».*