Investigadores de seguridad cibernética revelaron una campaña masiva que es responsable de inyectar código JavaScript malicioso en sitios web de WordPress comprometidos, que redirige a los visitantes a sitios web fraudulentos y otros sitios maliciosos para generar tráfico ilegítimo.

> *«Todos los sitios web compartían un problema común: se había inyectado JavaScript malicioso en los archivos y la base de datos de su sitio web, incluidos los archivos legítimos del núcleo de WordPress»,* dijo Krasimir Konov, analista de malware de Sucuri.

Esto ocasionó la infección de archivos como jquery.min.js y jquery-migrate.min.js con JavaScript ofuscado que se activa en cada carga de página, lo que permite al atacante redirigir a los visitantes del sitio web a un destino de su elección.

La compañía de seguridad de sitios web propiedad de GoDaddy, dijo que los dominios al final de la cadena de redirección podrían usarse para cargar anuncios, páginas de phishing, malware o incluso activar otro conjunto de redirecciones.

En algunos casos, los usuarios desprevenidos son llevados a una página de destino de redirección no autorizada que contiene una verificación de CAPTCHA falsa, al hacer clic se muestran anuncios no deseados que están disfrazados para parecer que provienen del sistema operativo y no de un navegador web.

La campaña, que es una continuación de otra ola que se detectó el mes pasado, afectó a 322 sitios web hasta ahora, desde el 9 de mayo. El conjunto de ataques de abril, ha violado la seguridad de más de 6500 sitios web.

> *«Se ha descubierto que los atacantes apuntan a múltiples vulnerabilidades en los complementos y temas de WordPress para comprometer al sitio web e inyectar sus scripts maliciosos»,* dijo Konov.