Los sitios de WordPress están siendo hackeados para mostrar páginas fraudulentas de protección DDoS de Cloudflare, que conducen a la entrega de malware como NetSupport RAT y Raccoon Stealer.

> *«Un aumento reciente en las inyecciones de JavaScript dirigidas a los sitios web de WordPress resultó en avisos falsos de prevención de DDoS que llevan a las víctimas a descargar malware troyano de acceso remoto»,* dijo Ben Martin de Sucuri.

Las páginas de protección de denegación de servicio distribuida (DDoS) son comprobaciones esenciales de verificación del navegador diseñadas para impedir que el tráfico malicioso y no deseado impulsado por un bot consuma ancho de banda y elimine sitios web.

El nuevo vector de ataque consiste en secuestrar sitios de WordPress para mostrar ventanas emergentes falsas de protección DDoS que, al hacer clic, conducen en última instancia a la descarga de un archivo ISO malicioso («security_install.iso») en los sistemas de la víctima.

Esto se logra mediante la inyección de tres líneas de código en un archivo JavaScript («jquery.min.js») o, alternativamente, en el archivo de tema activo del sitio web, que a su vez, carga JavaScript muy ofuscado desde un servidor remoto.

> *«Este JavaScript luego se comunica con un segundo dominio malicioso que carga más JavaScript que inicia el mensaje de descarga del archivo .iso malicioso»,* dijo Martin.

Después de la descarga, se solicita a los usuarios que ingresen un código de verificación generado desde la aplicación llamada *«DDoS Guard»* para atraer a la víctima a abrir el

archivo de instalación armado y acceder al sitio web de destino.

Aunque el instalador muestra un código de verificación para mantener la artimaña, en realidad, el archivo es un troyano de acceso remoto llamado NetSupport RAT, que está vinculado a la familia de malware FakeUpdates (también conocido como SocGholish) y también instala de forma encubierta Raccoon Stealer, un programa de robo de credenciales disponible para alquilar en foros clandestinos.

Este desarrollo es una señal de que los atacantes están cooptando de forma oportunista estos mecanismos de seguridad familiares en sus propias campañas en un intento por engañar a los visitantes del sitio web desprevenidos para que instalen malware.

Para mitigar dichas amenazas, los webmasters deben colocar sus sitios web detrás de un firewall, emplear controles de integridad de archivos y hacer cumplir la autenticación de dos factores (2FA). También es necesario que los visitantes del sitio web activen 2FA, evitar abrir archivos sospechosos y usar un bloqueador de secuencias de comandos en los navegadores web para evitar la ejecución de JavaScript.

> *«La computadora infectada podría usarse para robar redes sociales o credenciales bancarias, detonar ransomware o incluso atrapar a la víctima en una red 'esclava' maliciosa, extorsionar al propietario de la computadora y violar su privacidad, todo dependiendo de lo que decidan hacer los hackers con el dispositivo comprometido»,* dijo Martin.