Los sitios de WordPress están siendo atacados por una variedad previamente desconocida de malware de Linux que aprovecha las vulnerabilidades en más de dos docenas de plugins y temas para comprometer los sistemas vulnerables.

> *«Si los sitios usan versiones desactualizadas de dichos complementos, que carecen de soluciones cruciales, las páginas web seleccionadas se inyectan con JavaScripts maliciosos. Como resultado, cuando los usuarios hacen clic en cualquier área de una página atacada, son redirigidos a otros sitios»*, dijo el proveedor de seguridad ruso Doctor Web.

Los ataques implican armar una lista de vulnerabilidades de seguridad conocidas en 19 complementos y temas distintos que probablemente estén instalados en un sitio de WordPress, usándolo para implementar un implante que puede apuntar a un sitio web específico para expandir más la red.

También es capaz de inyectar código JavaScript recuperado de un servidor remoto para redirigir a los visitantes del sitio a un sitio web arbitrario elegido por el atacante.

Doctor Web dijo que identificó una segunda versión de la backdoor, que usa un nuevo dominio de comando y control C2, así como una lista actualizada de vulnerabilidades que abarca 11 plugins adicionales, lo que eleva el total a 30.

Los plugins y temas específicos son los siguientes:

- WP Live Chat Support
- Yuzo Related Posts
- Yellow Pencil Visual CSS Style Editor
- Easy WP SMTP
- WP GDPR Compliance
- Newspaper (CVE-2016-10972)
- Thim Core

- Smart Google Code Inserter (discontinued as of January 28, 2022)
- Total Donations
- Post Custom Templates Lite
- WP Quick Booking Manager
- Live Chat with Messenger Customer Chat by Zotabox
- Blog Designer
- WordPress Ultimate FAQ (CVE-2019-17232 and CVE-2019-17233)
- WP-Matomo Integration (WP-Piwik)
- ND Shortcodes
- WP Live Chat
- Coming Soon Page and Maintenance Mode
- Hybrid
- Brizy
- FV Flowplayer Video Player
- WooCommerce
- Coming Soon Page & Maintenance Mode
- Onetone
- Simple Fields
- Delucks SEO
- Poll, Survey, Form & Quiz Maker by OpinionStage
- Social Metrics Tracker
- WPeMatico RSS Feed Fetcher, and
- Rich Reviews

Se cree que ambas variantes incluyen un método no implementado para forzar cuentas de administrador de WordPress, aunque no está claro si es un remanente de una versión anterior o una funcionalidad que no se ha dado a conocer.

> *«Si se implementa dicha opción en las versiones más nuevas de la puerta trasera, los ciberdelincuentes incluso podrán atacar exitosamente algunos de esos sitios web que usan versiones actuales de plugins con vulnerabilidades parcheadas»,* dijo

> la compañía.

Se recomienda a los usuarios de WordPress que mantengan actualizados todos los componentes de la plataforma, incluidos los plugins y temas de terceros. También es recomendable usar nombres de usuario y contraseñas sólidos y únicos para proteger las cuentas.

La divulgación se produce semanas después de que Fortinet Fortiguard Labs detallara otra red de bots llamada GoTrim que está diseñada para forzar sitios web alojados por fuerza bruta usando el sistema de administración de contenido (CMS) de WordPress para tomar el control de los sistemas específicos.

El mes pasado, Sucuri notó que más de 15,000 sitios de WordPress habían sido violados como parte de una campaña maliciosa para redirigir a los visitantes a portales de preguntas y respuestas falsos. El número de contagios activos se sitúa actualmente en 9314.

La compañía de seguridad de sitios web propiedad de GoDaddy, en junio de 2022, también compartió información sobre un sistema de dirección de tráfico (TDS) conocido como Parrot que se ha observado apuntando a sitios de WordPress con JavaScript no autorizado que arroja malware adicional en sistemas hackeados.