Masterhacks – WordPress fue infectado por el malware wp-vcd, que que se distribuye mediante temas de la plataforma. Investigadores afirman que este malware sigue infectado a WordPress aún después de varios meses de haberlo detectado.

Esto es demasiado alarmante, pues el uso de WordPress en Internet es muy alto, cerca del 28% de las páginas web existentes utilizan este sistema de gestión de contenidos debido a su versatilidad y facilidad de uso, además de ser un proyecto de código abierto.

Manuel D´Orso, investigador italiano en seguridad, detectó este verano por primera vez al malware denominado como wp-vcd, que se oculta en archivos legítimos de WordPress para agregar un usuario administrador secreto y otorgar control a los atacantes en los sitios infectados. El malware también inyectaba código malicioso en los archivos principales como functions.php y class.wp.php.

WordPress había corregido este problema en las nuevas actualizaciones, pero últimamente, otro equipo de seguridad llamado Sucuri, detecto una nueva variación del malware, que inyecta código en algunos temas predeterminados de WordPress incluídos durante 2015 y 2016. Estos temas se encuentran instalados en muchos sitios web, ya que no muchos cambian su diseño con frecuencia.

Específicamente, los temas que se encuentran infectados son twentyfifteen y twentysixteen. El malware modifica los archivos y crea un administrador llamado 100010010, con el que se toma el control de la plataforma, pero según los investigadores, los ataques se concretaban en fechas posteriores.

El código es *«bastante directo y no oculta sus intenciones maliciosas mediante la codificación y ofuscación de funciones»*, dice uno de los informes. Los usuarios deben tomar precauciones y eliminar los temas mencionados en caso de tenerlos en su sitio web.