Miles Sitios Con WordPress, Joomla y Drupal Son Amenazados Por El Backdoor CryptoPHP

Una gran proporción de los sitios web están construidos sobre un **CMS en lugar de HTML puro**. Tres de los más comunes son WordPress, Joomla y Drupal, y los **investigadores de seguridad en Fox-It** advierten a los administradores del sitio que pueden encuentrarse en riesgo de ser de vulnerados mediante ingeniería social, con la instalación de la **puerta trasera CryptoPHP en su servidor**.

Este backdoor esta siendo distribuido a través de plantillas y plugins pirateados, la **propagación de CryptoPHP** se debe al manejo de los administradores. Este backdoor fue detectado por primera vez en 2013 y todavía se está extendiendo de forma activa. Las capacidades de la puerta trasera incluyen control remoto de un servidor infectado, y Blackhat SEO, por lo que tu sitio puede quedar valiendo nada después de la infección.

Fox-It advierte que miles de **sitios web han sido comprometidos por CryptoPHP**. La amenaza se llama así porque se utiliza la **criptografía de clave pública RSA** para proteger la comunicación con los servidores. Varias fuentes han sido asociados con la propagación del backdoor, como nulledstylez.com, pero muchos otros sitios intercambio de plugins y plantillas piratas están involucrados, incluyendo freemiumscripts.com, wp-nulled.com y mightywordpress.com.

Cada una de las descargas fue marcada por el sitio como libre de virus, pero Fox-It señala que las versiones disponibles

para su descarga diferían en que habían sido verificado como limpio por VirusTotal. Al examinar el contenido de las descargas piratas, se encontraron archivos con diferentes marcas de tiempo al resto incluyen la **puerta trasera oculta en el código PHP**.

El objetivo principal es **infectar sitios con WordPress, Joomla y Drupal**, y tiene bastante lógica, ya que estos son los CMS mas populares y usados por la mayoría de webmaster. La instalación del backdoor varía de una plataforma a otra, pero en el caso de WordPress se agrega una cuenta de administrador extra por lo que el acceso se puede mantener incluso si se retira la misma puerta trasera.

La actividad de CryptoPHP parece conducir a una dirección IP de Moldavia, específicamente en el estado de Chisinau. Los centros de control han sido identificados en el, Polonia, Alemania y Países Bajos Estados Unidos y Fox-It ha lanzado un documento que detalla la forma de detectar la presencia de este peligroso backdoor.