

# ¿Cómo evitar ser víctima de los hackers?

escrito por Andy Garcia | 18/02/2016

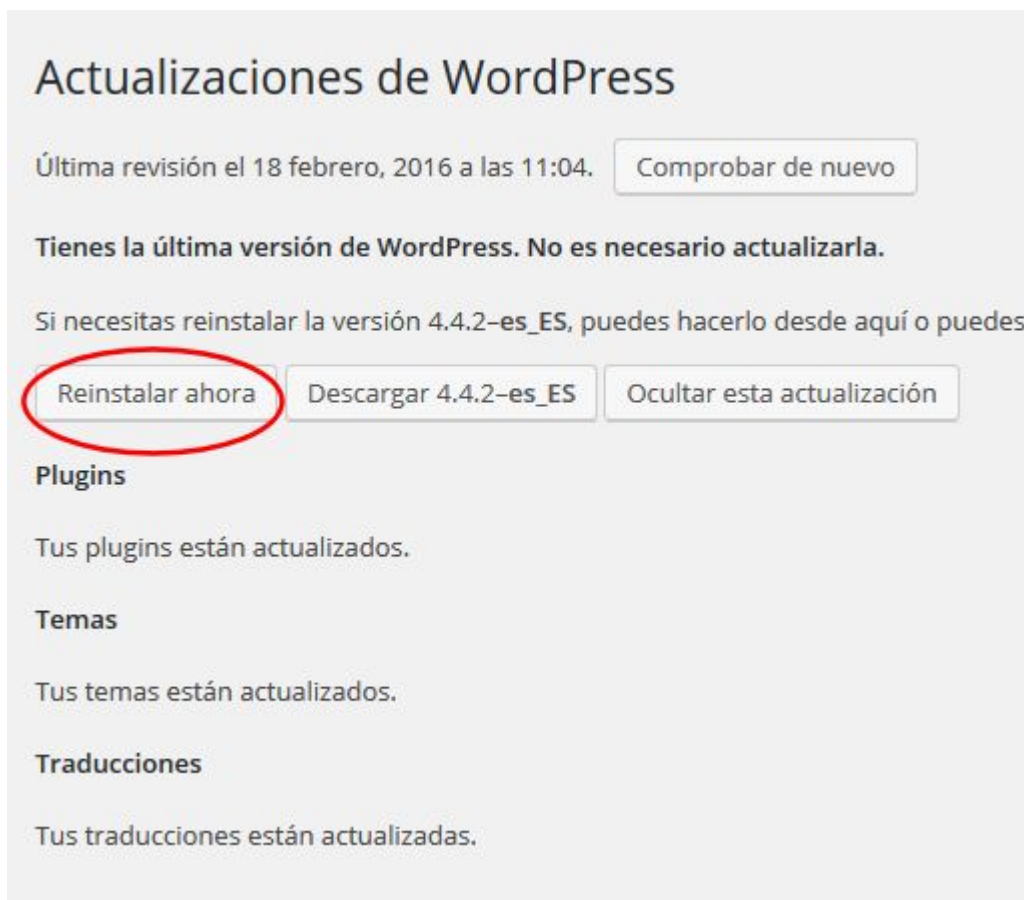


Después de «*divertirme*» defendiendo un [servidor VPS](#) de **ataques de hackers**, hace casi una semana de la última batalla y doy la guerra por prácticamente ganada, ahora estas son las conclusiones:

- Los CMS más antiguos (por ejemplo Joomla 1.5), en contra de lo que podía parecer NO son los más vulnerables, ya que los hackers no se sienten motivados a penetrar semejantes «reliquias».
- El CMS más vulnerable ha sido Joomla, precisamente en su versión más actualizada, la 3.4.8, he tenido

intrusiones también en WordPress y Drupal pero las más numerosas con diferencia han sido las de Joomla.

- **Sólo WordPress tiene una función en su backend para reinstalarse**, aunque lo tengas actualizado, con un sólo clic puedes sobre-escribir todos los archivos limpios desde el repositorio oficial, con Drupal y Joomla también se puede hacer pero usando herramientas de terceros o a mano.



The screenshot shows the 'Actualizaciones de WordPress' (WordPress Updates) section. At the top, it states 'Última revisión el 18 febrero, 2016 a las 11:04.' with a 'Comprobar de nuevo' button. Below this, it says 'Tienes la última versión de WordPress. No es necesario actualizarla.' (You have the latest version of WordPress. It is not necessary to update it.). A message follows: 'Si necesitas reinstalar la versión 4.4.2-es\_ES, puedes hacerlo desde aquí o puedes' (If you need to reinstall version 4.4.2-es\_ES, you can do it from here or you can). Three buttons are displayed: 'Reinstalar ahora' (highlighted with a red circle), 'Descargar 4.4.2-es\_ES', and 'Ocultar esta actualización'. Below the buttons, there are sections for 'Plugins' (Tus plugins están actualizados.), 'Temas' (Tus temas están actualizados.), and 'Traducciones' (Tus traducciones están actualizadas.).

*Plesk tiene módulos que te ayudan a prevenir ataques y a luchar contra ellos si se producen, sólo hay que instalarlos y configurarlos, se trata de «fail2ban» y «ModSecurity».*

Uno de los ataques más frecuentes consiste en **tomar el control de tu servidor de e-mail** y enviar (de forma remota) miles de correos de spam por hora desde tu servidor infectado, aprox. en 24 horas tendrás tu IP en listas

negras y no podrás enviar e-mails legítimos, esto se hubiera evitado activando límites a los correos salientes, en Plesk 12.0 o superior es muy fácil y puedes activar también una notificación que te avisará si uno de los límites es superado.



*Si hay cosas que no usas, por ejemplo las listas de correo (mailman), mejor desactivar o desinstalar el módulo correspondiente.*

Mi nivel de conocimientos de Plesk y **defensa anti-hackers** se ha multiplicado por 3 durante las 3 últimas semanas, estoy encantado de haber «luchado» en esta guerra, he perdido algunos «hombres» pero mi «ejercito» es ahora más fuerte que nunca.

*Los detalles de cada batalla y la configuración de las herramientas utilizadas se sale del propósito de este post, me reservo esa información para la publicación de futuros post más técnicos.*

Si tu web te va muy lenta y no sabes el motivo, seguramente será que tienes troyanos robando tu ancho de banda o incluso tu dinero si tu web es de eCommerce, es decir, eres victima de los hackers.