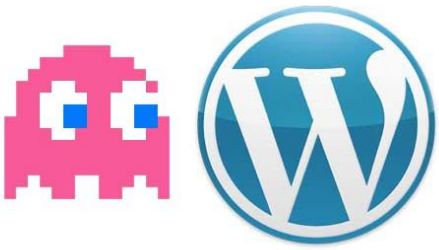
Limpiar de malware nuestro sitio de WordPress infectado



WordPress se ha convertido en una de las herramientas más utilizadas a nivel mundial a la hora de crear una página web gracias a la gran cantidad de plantillas y plugins que proporciona, que permiten hacer prácticamente cualquier cosa. Pero este éxito también ha traído consigo que las vulnerabilidades del código habiliten a los atacantes a infectar nuestro sitio. Ante esta situación, sólo queda remangarse la camisa y ponerse manos a la obra para solucionar el problema. A lo largo de este White Paper veremos cómo localizar esas amenazas y acabar con ellas.

Prevenir antes que lamentar

La parte más importante para estar protegidos ante cualquier tipo de amenaza es la prevención, lo que se traduce en que debemos realizar determinadas acciones para evitar dentro de lo posible que nuestro sitio web sea infectado.

La principal acción que deberían realizar los usuarios de WordPress es la de tener siempre su sitio actualizado con la última versión estable disponible, una versión que suele solucionar agujeros de seguridad detectados en versiones anteriores. Además de esto, también es muy importante hacer lo mismo con los plugins que utilicemos, así como eliminar todos aquellos que no utilicemos.

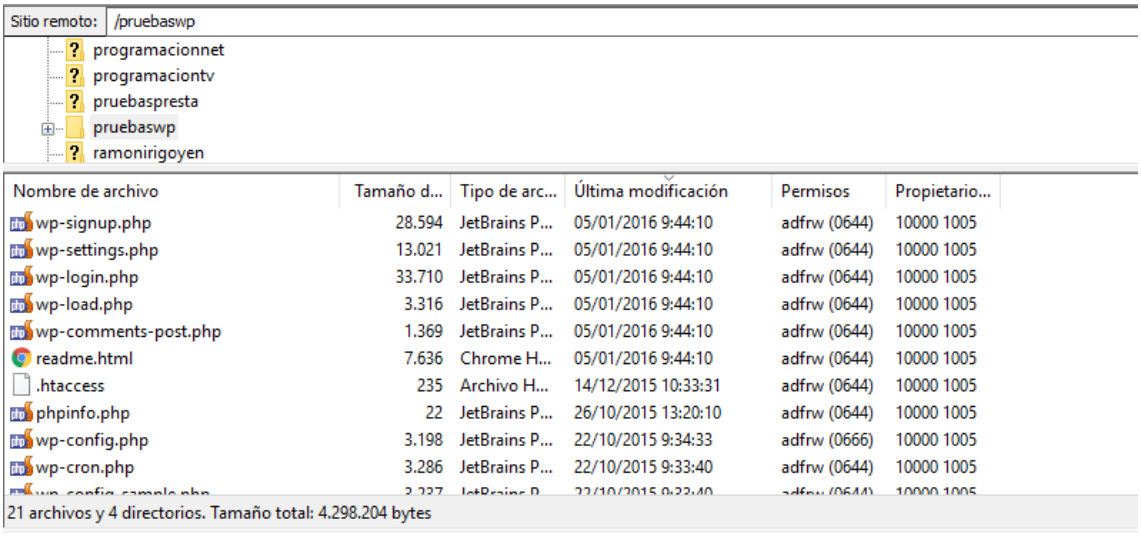
Cuando un malware entra en un sitio, son muchas las cosas que pueden ocurrir, pero lo que está claro es que ninguna de ellas es buena. Entre los problemas que pueden aparecer están:

- Aumentar el consumo de recursos del servidor, tanto web como MySQL
- Robo de datos personales de usuarios y clientes
- Penalización por parte de Google
- Mensajes de alerta de que nuestro sitio está infectado
- Aparición de publicidad no deseada
- Envío de correo spam de forma masiva
- Desaparición de la información de nuestro sitio

Cómo detectar el malware y los archivos infectados

Una vez que nos hemos dado cuenta de que nuestro sitio ha sido infectado con algún tipo de código malicioso, lo primero que debemos hacer es detectar qué tipo de malware nos ha infectado y qué archivos son los que se encuentras infectados. Para conseguir este objetivo, podemos hacer uso de varias opciones.

1.- Listar archivos por fecha de modificación



Una de las formas más rápidas de detectar los archivos potencialmente peligrosos es acceder vía FTP y ordenarlos por fecha de modificación. De esta forma, en los primeros lugares aparecerán aquellos que han sufrido algún tipo de cambio recientemente. Si nosotros no hemos cambiado nada en ellos, puede ser síntoma de que en su interior haya algún tipo de código que esté causando el problema. El problema de este sistema, es que habría que recorrerse todas las carpetas que forman parte del sitio para localizar cada uno de los archivos infectados, un trabajo que podría ser muy tedioso si el código ha sido insertado en un elevado número de ficheros.

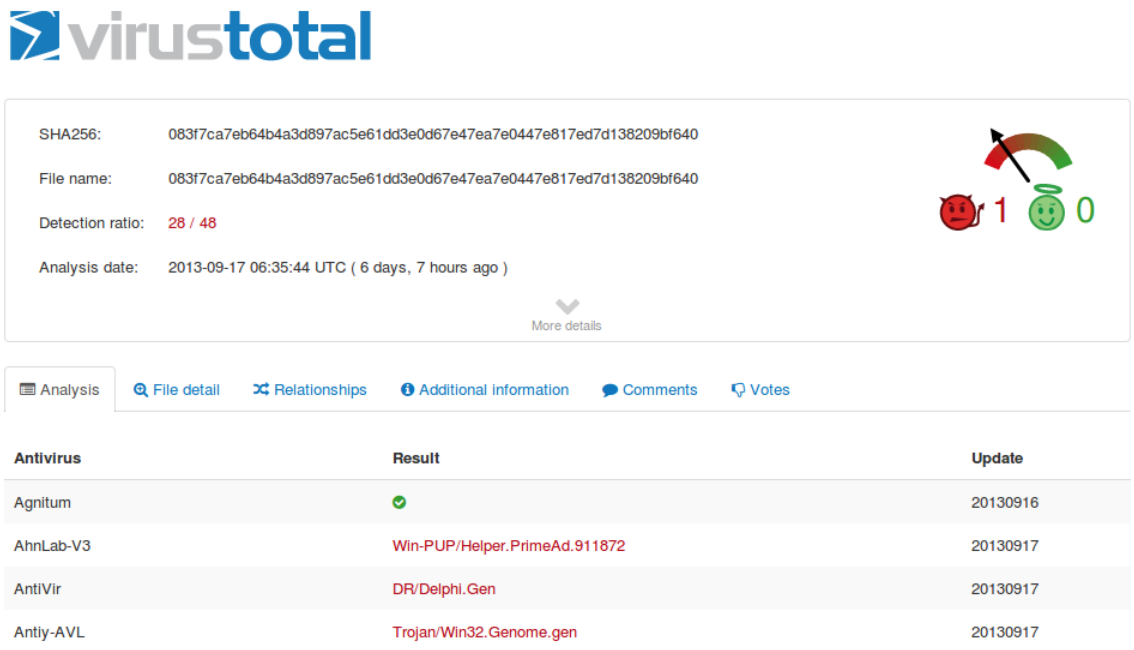
2.- Analizar con un antivirus instalado en nuestro equipo informático

Otra de las opciones que podemos utilizar para detectar los archivos que han sido infectados es hacer uso de algún antivirus que tengamos instalado en nuestro ordenador. Con un programa FTP nos podemos

descargar todo el sitio para que cada uno de los archivos que forman parte de la web sea analizado en busca de código malicioso.

Normalmente los antivirus son capaces de analizar los archivos mientras se van descargando, por lo que una vez completada la descarga sólo deberíamos ir a ver el informe generado para conocer cuáles son los que han sido señalados como potencialmente peligrosos.

3.- Escanear el sitio online



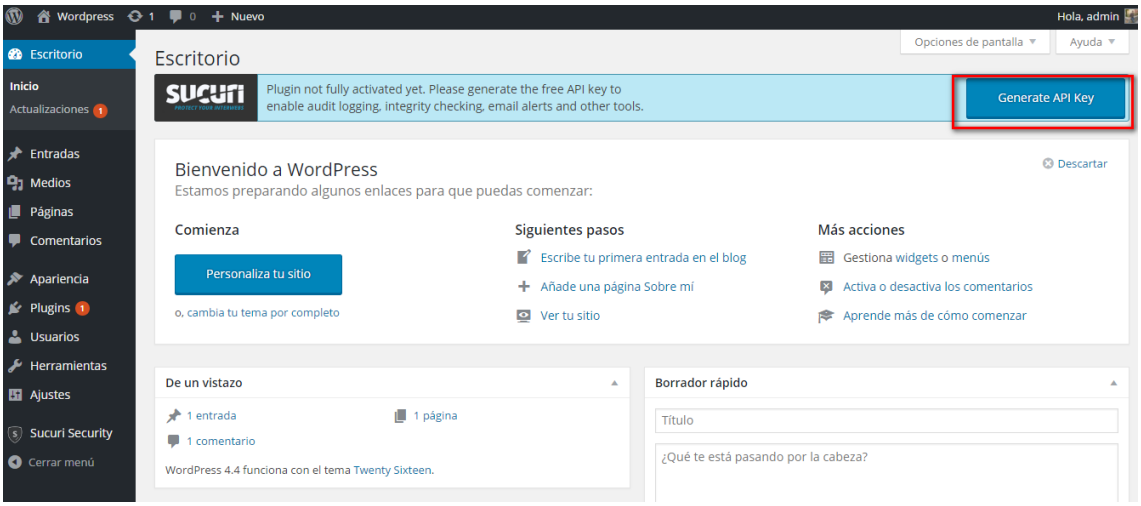
Si las opciones anteriores no han dado buenos resultados o no te gustan, siempre podemos utilizar alguna de las herramientas online que nos podemos encontrar por la red y que son capaces de realizar un escaneo de nuestro sitio en busca de malware. Entre las aplicaciones de este tipo más conocidas podemos destacar: Virustotal, Quttera, Google, Sucuri...

Una vez que ha sido analizado todo nuestro sitio, estas herramientas muestran un informe con los archivos que han sido infectados.

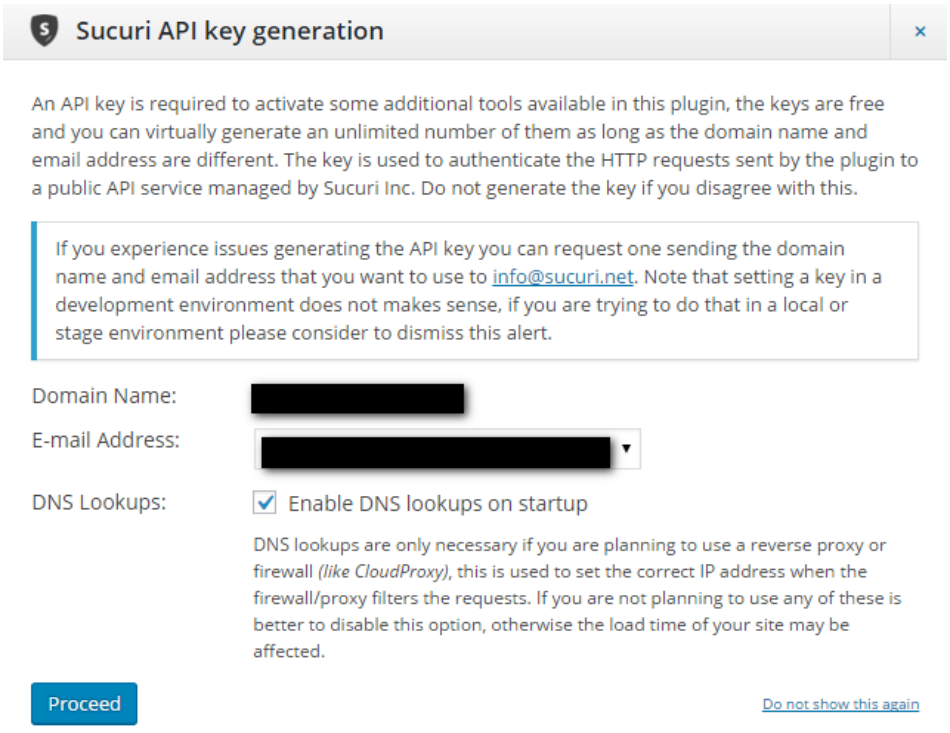
Dentro de las herramientas online también podemos activar la herramienta Webmaster de Google para consultar su sección de "**Problemas de seguridad**" donde nos informará del tipo de amenaza que estamos sufriendo.

4.- Escanear mediante el uso de plugins

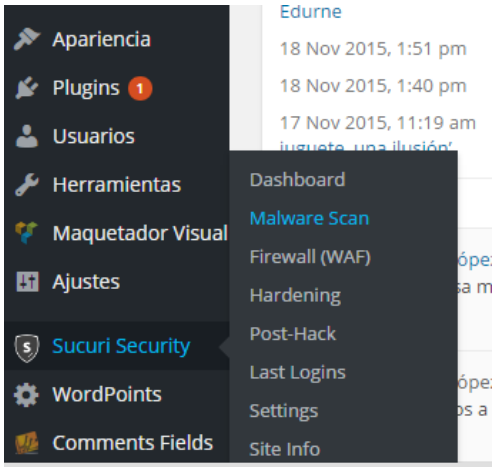
Como todo el mundo sabe, si hay algo que diferencia a WordPress del resto de CMS es la gran comunidad de desarrolladores que tiene detrás de él, lo que permite encontrar nuevas funcionalidades que instalar en nuestro sitio por medio de plugins. Esto hace que también sea posible encontrarnos uno de estos plugins que nos ayude a localizar los archivos que han sido infectados. Es el caso de Sucuri Security, un añadido que una vez instalado y generada la clave para su funcionamiento nos ayudará a conseguir nuestro objetivo.



Para conseguir la "**API Key**" para el funcionamiento del producto, lo primero sería instalarlo como hacemos con cualquier otro plugin, y una vez que lo tengamos activado, pulsaremos en el botón que nos aparecerá en nuestro escritorio de WordPress y que pone "**Generate API Key**".

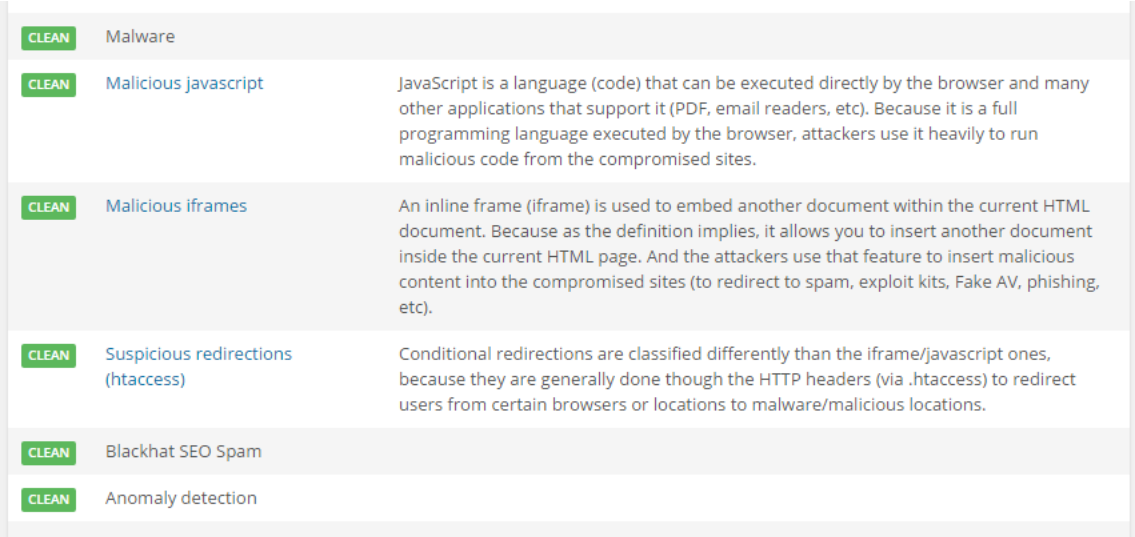


En la ventana que nos aparecerá, pulsaremos el botón de "**Proceed**" y esperaremos a que el proceso finalice.



Una vez que lo tengamos completamente activado, para realizar una revisión de nuestro sitio debemos elegir la opción "**Malware Scan**" dentro del menú "**Sucuri Security**" que nos aparecerá en nuestro escritorio.

Por último sólo faltaría pulsar el botón "Scan Website" para que empezase el proceso.



Una vez finalizado, el plugin nos mostrará un informe con los resultados. En nuestro caso, nos informa de que no tenemos ningún tipo de amenaza en nuestro código.

No penséis que este es el único plugin que nos podemos encontrar para este fin, sino que hay otros como WP Antivirus Site Protection, Anti-Malware Security and Brute-Force Protection o Quttera Web Malware Scanner.

Estoy infectado, ¿cómo actúo para eliminar el malware?

Una vez que hemos detectado el código malicioso y para evitar mayores problemas a los usuarios que visiten nuestro sitio, lo que podemos hacer es poner la web en "modo de mantenimiento" mostrando un mensaje avisando de la situación, o bien creando en el archivo .htaccess una nueva regla que bloquee el acceso al portal.

Ahora que tenemos localizados los archivos que han sido infectados, la pregunta es: ¿cómo hacemos esto? La respuesta en este caso varía dependiendo del tipo de hackeo que hayamos sufrido, pero la idea principal es eliminar o limpiar de código malicioso los archivos.

El primer paso que debemos hacer es borrar todo archivo que haya sido infectado, que sea sospechoso o que no forme parte de la instalación de WordPress, plugins instalados o plantilla utilizada y que no haya sido subido por nosotros. Ante cualquier duda, podemos realizar una búsqueda por Internet para ver si realmente ese archivo forma parte de la programación del CMS o no.

El problema puede aparecer cuando ha sido marcado como archivo potencialmente peligroso un fichero que forma parte de WordPress, de algún plugin o del tema. En este caso tenemos dos opciones:

- Sustituir los archivos infectados por archivos nuevos limpios de malware
- Editar esos archivos con código malicioso y eliminar ese código

En muchas ocasiones, la segunda opción puede ser complicada sobre todo para aquellos que no son expertos en programación. De todas, puede servir de pista que este tipo de código que inyectan en los archivos los atacantes suelen utilizar las directivas **base64_decode y eval,** aunque siempre nos podemos encontrar con falsos positivos, por lo que hay que tener mucho cuidado con lo que eliminamos.

Para evitar esta situación, nuestra recomendación es que se haga una sustitución completa de todos los archivos en el servidor. De esta forma nos garantizamos acabar con todo el código malicioso, incluido aquel que no haya sido localizado. También recomendamos que en vez de sustituir lo que se haga sea borrarlos y volver a subirlos vía FTP siguiendo los siguientes pasos.

- Sustituir los archivos de WordPress por los descargados del sitio oficial teniendo en cuenta utilizar siempre la misma versión que teníamos instalada, para evitar incompatibilidad con la base de datos
- Borrar la carpeta "wp-content/plugins" y crear una nueva carpeta vacía "plugins" dentro del directorio "wp-content". Descargar cada uno de los plugins que estemos utilizando de su sitio oficial y subirlos descomprimidos a esa nueva carpeta que hemos creado
- Repetir el paso anterior con la plantilla que estemos utilizando en nuestro sitio

Buenas prácticas en WordPress para una mayor seguridad

Para garantizar una mayor seguridad de nuestro CMS, es recomendable llevar a cabo una serie de prácticas para fortalecer nuestro sitio. Entre estas prácticas podemos destacar:

- Realizar copias de seguridad periódicas tanto de los archivos que forman parte de la web como de la base de datos del sitio
- Reducir al mínimo el número de plugins utilizados y eliminar aquellos que no utilicemos
- Hacer uso de contraseñas robustas tanto para el acceso a la administración, como para la cuenta FTP y base de datos
- Aplicar protección extra utilizando para ello directivas del archivo .htaccess
- Mantener el core de Wordpress, los plugins y el tema utilizado, actualizado a la última versión estable disponible
- Descargar plugins y temas de sitios de confianza

Si somos capaces de llevar a cabo este tipo de acciones, podremos disfrutar de una instalación de WordPress mucho más segura.