

# General: Alertas de Malware o Virus por acciones de Code Injection en los servicios -Causas y Soluciones

*Este documento tiene informacion acerca Alertas de Malware o Virus por acciones de Code Injection que pueden aparecer en los servicios de hospedaje y generar que su sitio sea registrado como un sitio inseguro o potencialmente peligroso*

Informacion y consejos de solucion sobre sitios no seguros infectados con alguacute;n tipo de Malware en el siguiente v&iacute;nculo:

[http://www.viafacil.com/faq/content/6/232/es/malware-\\_-mi-p%E1gina-figura-como-un-sitio-no-seguro-en-los-buscadores-de-internet-google-yahoo-etc.html](http://www.viafacil.com/faq/content/6/232/es/malware-_-mi-p%E1gina-figura-como-un-sitio-no-seguro-en-los-buscadores-de-internet-google-yahoo-etc.html)

&iquest;De qu&eacute; manera llega el malware con capacidades de Code Injection a mi servicio?

El atacante o el Cracker modifica el c&acute;digo de tus p&acute;ginas (principalmente el index) con una metodolog&iacute;a que se conoce como "iframe attack&rdquo;. Le suma l&iacute;neas de c&acute;digo que lo que hacen es llamar a otra p&acute;gina, sin que quienes visiten tu sitio lo noten, con la intenci&acute;n de posicionarla mejor o bien infectar con virus las PCs de tus clientes y visitantes.

Las formas m&acute;s comunes de infectar un sitio son dos: alojando el virus en tu equipo o interceptando los archivos al momento de subirlos por FTP. Si el malware est&acute; en tu equipo, va a robar tus claves del FTP y las va a usar para subir por su cuenta los archivos infectados. En el segundo caso, detecta el momento en que te est&acute;s conectando por FTP, toma tus claves y las usa para subir los archivos modificados.

Este tipo de problemas generalmente es causado por un tipo de actividad ilegal denominada code injection (inyecc&iacute;n de c&acute;digo), el cual es inyectado en sus p&acute;ginas webs vali&eacute;ndose de vulnerabilidades en sus aplicaciones php, java script, o el mismo c&acute;digo html

Alertas de virus en los servicios y ataques mediante Code injection

**&iquest;C&acute;mo ingres&acute; el virus en su servicio?**

A diferencia de lo que indicar&iacute;a el sentido com&uacute;n (&rdquo;si mi sitio tiene un virus, est&acute; infectado el servidor web de mi proveedor de hosting&rdquo;), el problema casi siempre est&acute;/estuvo en la PC desde donde se actualiza el sitio web.

Quienes se dedican a subir este tipo de virus, con la intenci&acute;n de expandirlos a trav&eacute;s de internet, apuntan a robar una informaci&acute;n fundamental: sus claves FTP.

Con esas claves, suben archivos infectados o sus p&acute;ginas modificadas, sin que Ud. se d&eacute; cuenta. Es m&acute;s, si el ataque es lo suficientemente elaborado, hasta conseguir&acute;n al instante su nueva clave de FTP en el momento que la modifique.

Otra manera muy com&uacute;n de agregar un virus o c&acute;digo malicioso a un sitio es

*P&acute;gina 1/4*

(c) 2010 Viafacil.com - servicios inform&acute;ticos. <mzanlongo@gmail.com>

URL: [http://www.viafacil.com/content/6/305/es/alertas-de-malware-o-virus-por-acciones-de-code-injection-en-los-servicios-\\_causas-y-soluciones.html](http://www.viafacil.com/content/6/305/es/alertas-de-malware-o-virus-por-acciones-de-code-injection-en-los-servicios-_causas-y-soluciones.html)

# General: Alertas de Malware o Virus por acciones de Code Injection en los servicios -Causas y Soluciones

explotando la vulnerabilidad de una aplicación desactualizada (foro, blog, galería de fotos, carrito de compras, etc.). Por eso es fundamental tener siempre la aplicación actualizada y aplicar los parches de seguridad recomendados por sus desarrolladores.

## ¿Cómo encuentro el virus?

La forma más usada para esconder un virus en un sitio web se conoce como "iframe attack";

El "iframe" se esconde en el código de sus páginas, y lo que hace es llamar a otra página de forma invisible (es decir, ni Ud. ni quien visite su web lo notan), buscando posicionar mejor esa página escondida o bien infectar con virus o código malicioso a los visitantes.

Lo más común es que lo agreguen al código de su página index (index.html, index.php, etc.). También ocurre, con virus como Gumblar.cn, que suban un archivo y lo ubiquen en una carpeta donde sea difícil detectarlo (Gumblar.cn, por ejemplo, sube un archivo llamado "image.php" dentro de la carpeta "images").

## ¿Cómo eliminar el virus o la alerta de virus en su servicio?

- 1) Ingresar por FTP y descargar todo el contenido del sitio a una carpeta dentro de su equipo. Inmediatamente después, cambiar la contraseña del FTP desde su Panel de control Plesk o su Panel de Control HELM
- 2) Correr un buen antivirus y antispyware en la carpeta de su equipo local que contiene la web, y en el resto del equipo (incluyendo discos extraíbles).
- 3) Una vez que el antivirus haya eliminado archivos sospechosos, comienza el trabajo manual dentro de la carpeta donde está su web.

Con un programa que permita buscar dentro de los archivos, habrá que identificar todos aquellos que incluyan un "iframe" con estilo escondido ("hidden"), que no correspondan a su página, y eliminar esa porción de código.

## Ejemplo de código sospechoso:

```
style="visibility: hidden; display: none";>
```

Implementando el mismo procedimiento, buscar también si en alguna página existe un "document.write", seguido de una línea encodeada.

## Ejemplo de código sospechoso:

```
document.write( unescape( '%70%61%67%65%20%6F%6E%65' ) );
```

Página 2/4

# General: Alertas de Malware o Virus por acciones de Code Injection en los servicios -Causas y Soluciones

**Recuerde:** Si ud ubica alguna de las piezas de código indicadas en los ejemplos anteriores, elimínelas.

Asegúrese que todos los src= y http:// hagan referencia a archivos de su sitio web o a sitios externos que Ud. conoce y son confiables.

Se recomienda que también efectúe una revisión manual para buscar entre todos los archivos la existencia de cualquier .php, .js, .htm, .html, asp, .aspx, .inc, .cfm, etc., que no pertenezca a su sitio web.

4) Una vez hecho esto, ya seguro de que su sitio está limpio, contáctese por FTP a su servicio. Elimine todo el contenido de la carpeta httpdocs (Plesk) wwwroot (Helm) u public\_html (cPanel) , y suba los archivos que acaba de limpiar.

A modo preventivo: Recomendamos que utilice contraseñas que incorporen caracteres especiales , debido a que contraseñas simples como "Pedro" o sucesiones de letras de su teclado, como los números "123456" u "qwerty" ingresadas en orden de escritura de izquierda a derecha o derecha a izquierda ("ytrewq" u "654321"), son fácilmente descifradas por aplicaciones maliciosas. Implemente contraseñas con combinaciones de letras, números y al menos un carácter especial.

5) Ahora, elimine el caché de su navegador (para ver un instructivo haga click aquí), abra la página index de su web y todas aquellas que detecte como infectadas en la primera revisión.

Del menú del browser elija la opción para ver el código fuente de cada página. Si no aparece más el "iframe" que apunta a una web desconocida o el "document.write", entonces significa que el sitio está limpio.

6) Si Google marca su web como sospechosa, será necesario que solicite una revisión para levantar la página de alerta. Deberá completar el formulario en **Google Webmaster Central** o **StopBadware**.

Nota: Recuerde que la página de advertencia que muestra Google ( u cualquier otro buscador) al intentar ingresar a su sitio, desaparecerá dentro del transcurso de 7 días cuando Google vuelva a analizar el contenido de su sitio Web.

Links de utilidad:

- **Google Webmaster Central:** <http://www.google.com/webmasters/>
- **StopBadware:** <http://www.stopbadware.org/home/reviewinfo>

# *General: Alertas de Malware o Virus por acciones de Code Injection en los servicios -Causas y Soluciones*

*Solución única ID: #1291*

*Autor: : helpdesk*

*Última actualización: 2010-03-01 19:49*