Google Webmasters Y Los Sitios Hackeados

Tener su **sitio web hackeado** puede ser una experiencia frustrante y queremos hacer todo lo posible para ayudar a los **webmasters** a tener sus sitios limpios y evitar que sucedan futuros compromisos de seguridad. Con este post hemos querido esbozar dos tipos comunes de ataques, así como proporcionar las medidas de limpieza y los recursos adicionales que los webmasters pueden resultarle útiles.

Para servir mejor a los usuarios es importante que las páginas que enlazan a los resultados de búsqueda son seguros para visitar.

Desafortunadamente, terceras personas malintencionadas, **podrán hackear sus sitios** para manipular los resultados del motor de búsqueda o distribuir contenido malicioso y spam. Google va alertar a los usuarios y webmasters por igual al etiquetar sitios que han detectado como "**hacked by**" y mostrar una etiqueta de advertencia en los resultados de búsqueda que dice "**Este sitio puede ser peligroso**".

Example site
www.example.com
This site may be compromised.
Example site snippet...

Queremos dar a los **webmasters** la información necesaria para ayudarles a limpiar sus sitios tan pronto como sea posible. Si has verificado su sitio en las Herramientas para webmasters de

Google, esta también enviará un mensaje cuando han identificado que su sitio ha sido hackeado, y cuando sea posible puede darle un ejemplo de una URL.
De vez en cuando, su sitio puede estar comprometido para facilitar la distribución de malware. Cuando google se da cuenta de eso, va a identificar y marcar el sitio en los resultados de búsqueda con la etiqueta de “Este sitio puede dañar tu equipo” y en los navegadores como Chrome puede mostrar una advertencia cuando los usuarios intenten visitar su sitio web. En algunos casos, es posible que exista información más específica en la sección de malware de Herramientas para webmasters de google. También google cuenta con consejos específicos para prevenir y eliminar el malware de su sitio en el Centro de asistencia.

Dos formas comunes de malware que puedan comprometer su sitio son los siguientes:

El Contenido Injected

Los hackers pueden intentar influir en los motores de búsqueda mediante la inyección de enlaces que conducen a sitios que poseen. Estos enlaces se ocultan a menudo para que sea difícil para un webmaster detectar esto ny donde ha ocurrido. El sitio también puede verse comprometido de tal manera que el contenido sólo se muestra cuando el sitio es visitado por los rastreadores de motores de búsqueda.

cialis once a day online
20 mg cialis split in 4ths and taken daily
generic cialis quick delivery
cialis stays in the system
cialis storage refrigerator

- generic viagra 25mg
- generic viagra online au
- canada propecia no prescription
- cialis 40 mg online
- buy accutane online
- lisinopril price
- viagra professional generic

Redirigir Usuarios

Los hackers también podrían tratar de redirigir a los usuarios a sitios maliciosos o de spam. Pueden hacerlo a todos los usuarios o usuarios específicos, tales como los procedentes de los motores de búsqueda o aquellos en los dispositivos móviles. Si usted es capaz de acceder a su sitio cuando lo visite directamente experimenta redireccionamientos inesperados cuando proviene de un motor de búsqueda, es muy probable que su sitio ha sido comprometido de esta manera.

Una de las maneras de lograr esto consiste en modificar los archivos de configuración del servidor (por ejemplo,. Htaccess de Apache) para mostrar contenidos diferentes a los usuarios, así que es una buena idea verificar sus archivos de configuración del servidor para cualquier modificación.

```
RewriteCond %{HTTP_REFERER} ^.*(google|ask|yahoo|baidu|msn)\.(.*)
RewriteRule ^(.*)$ http://[ spammy redirect destination] [R,L]
```

Archivo .htaccess con código malicioso.

Este comportamiento malicioso también puede llevarse a cabo mediante la inyección de JavaScript en el código fuente de su sitio. El código JavaScript se puede diseñar para ocultar su propósito por lo que puede ayudar a buscar términos como

*“**eval**“*, *“**decode**”* y *“**escape**“*.

```
eval(function(p,a,c,k,e,r){e=function(c){return(c<a?'
String.fromCharCode(c+29):c.toString(36))};if(!''.rep
[c]||e(c);k=[function(e){return
r[e]}];e=function(){return'\\w+'};c=1};while(c--)if(k
RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('o
r=a.e,t="",q;5(r.4("m.")!=-1)t="q";5(r.4("b.")!=-1)t=
!=-1)t="q";5(r.4("g.")!=-1)t="h";5(r.4("i.")!=-1)t="c
r.4("&"+t+"="))!=-1))j.k="l://9"+"1."+"n"+"3"+"."+"8"
y="+r.z(q+2+t.6).A("&")[0];',37,37,'||||indexOf|if|le
altavista|aol|query|ask|window|location|http|google|2
|split'.split('|'),0,{}))
```

Inyección de funciones con código malicioso en JavaScript

Limpieza Y Prevención

Si su sitio ha sido comprometido, es importante no solo limpiar los cambios realizados en los archivos de su sitio sino para tratar también la vulnerabilidad que permitió que el ingreso no autorizado de **malware**.

Google webmaster ofrece instrucciones para la limpieza de su sitio y evitar ataques, mientras que el soporte técnico de su proveedor de alojamiento y las herramientas de google webmaster son excelentes recursos si necesita asesoramiento más específico.

Una vez que haya limpiado su sitio usted debe presentar una solicitud de reconsideración a google webmaster, que si tiene éxito, va a quitar la etiqueta de advertencia en nuestros resultados de búsqueda.