Secuestradores del navegador, qué son y cómo combatirlos

Una compañía de Telefónica

acens
the Cloud services company

Introducción

Todos estaremos de acuerdo en que el desarrollo de Internet nos ha ayudado mucho en nuestras tareas cotidianas. Hoy en día prácticamente todo lo que se nos ocurra lo podemos hacer desde cualquier dispositivo conectado a la red, desde buscar información sobre cualquier cosa hasta registrar un nombre de dominio para nuestra página web, o simplemente estar en contacto con aquella persona que está a miles de kilómetros de distancia.

Pero este desarrollo de Internet también ha traído la aparición de amenazas que ponen en riesgo nuestra información, que pueden darnos más de un quebradero de cabeza si no tomamos las medidas necesarias: virus, troyanos, spyware… están a la orden del día.

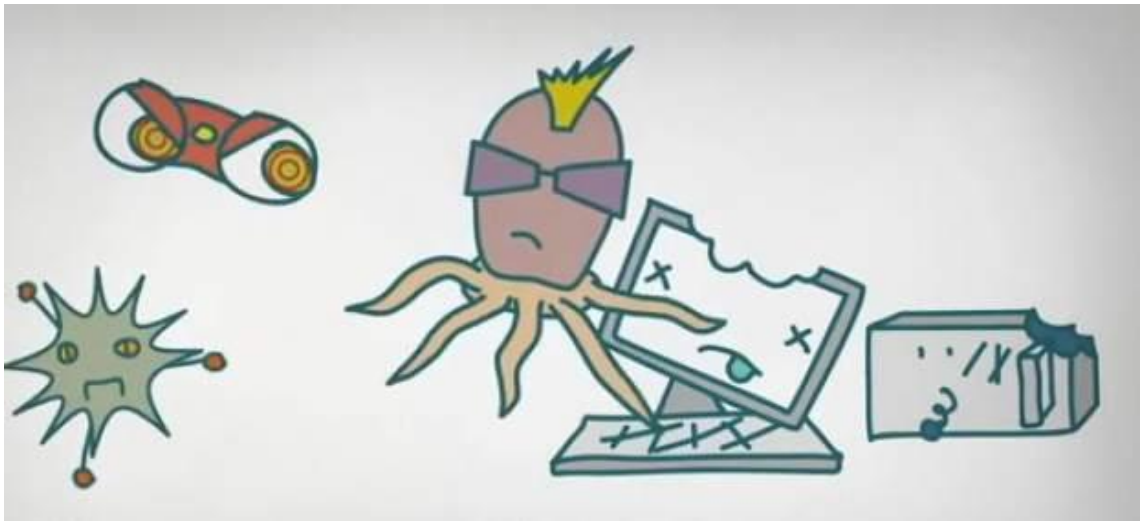
Hoy en nuestro White Paper nos centraremos en una amenaza que puede ser menos conocida que las citadas anteriormente, pero que puede llegar a ser muy molestas. Nos estamos refiriendo a los Browser Hijackers, o traducidos al castellano "Secuestradores del navegador".

Qué son los secuestradores de Internet

Los Browser Hijackers o secuestradores del navegador son un tipo de malware que lleva activo desde el primer día que aparecieron los exploradores web. Suele tratarse de ataques poco peligrosos, ya que no es habitual que roben información o realicen estafas al usuario, aunque sí pueden redirigirnos a otras páginas que realicen este tipo de prácticas.

Cuando un equipo informático es atacado por uno de estos secuestradores del navegador, éste suele alterar la página inicial del browser impidiendo al usuario cambiarla. Otra de las acciones habituales que suelen realizar es la de mostrar publicidad dudosa mediante el uso de pop-ups, instalar barras de herramientas en el navegador, bloquear el acceso a determinadas páginas web (sobre todo a webs relacionadas son software antivirus) y en los casos más extremos pueden llegar a falsear las búsquedas que hagamos en Google o cualquier otro buscador.

Cómo se cuelan en tu equipo



Como suele ocurrir con la mayoría de las amenazas que nos podemos encontrar hoy en día circulando por la red, la forma habitual que tienen estas amenazas para infectar los equipos de los usuarios es mediante la descarga de un programa desde una página no oficial, en la que el atacante ha camuflado el hijacker. Normalmente suele darse con páginas de juegos o de contenido adulto, donde se pide expresamente la instalación de algún software para la correcta visualización del contenido.

Una vez que hayamos instalado el software en nuestro equipo, el hijacker toma el control del navegador impidiendo al usuario su funcionamiento habitual.

Cómo saber si tu explorador ha sido asaltado

Aunque hayamos comentado anteriormente que este tipo de ataques no suelen ser muy peligrosos, sí que suelen ser muy molestos para los usuarios debido a las acciones que realizan en el equipo. A continuación os explicaremos algunos síntomas que nos pueden ayudar a pensar que nuestro equipo está infectado con una de estas amenazas.

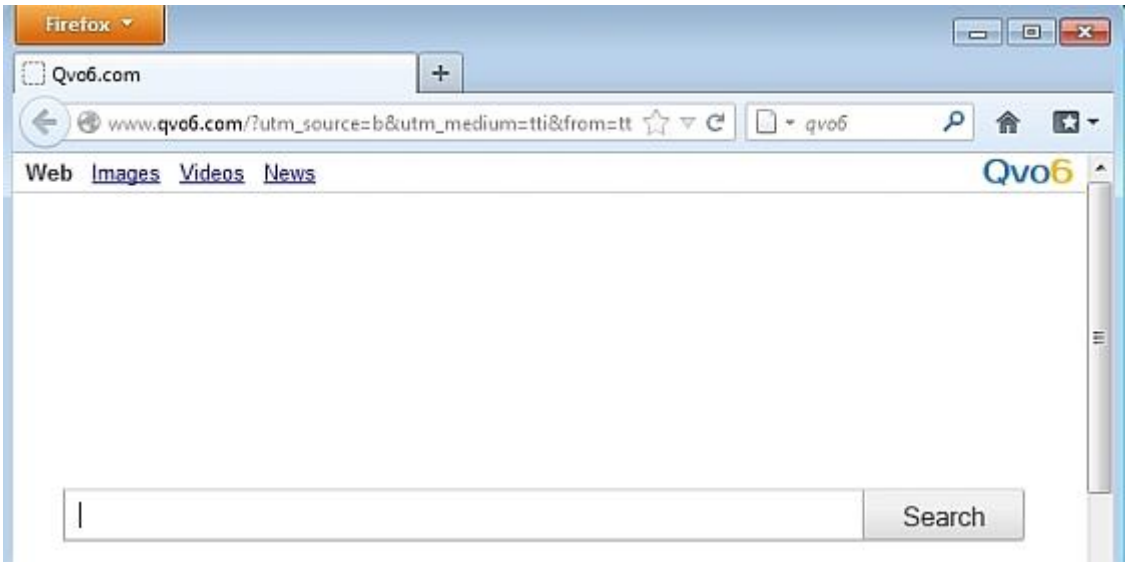
- Se cambian la página principal del navegador y otras configuraciones del equipo, impidiendo que se vuelvan a modificar.
- Se bloquea el acceso a determinadas páginas web, sobre todo portales de software de seguridad.
- Se produce un bombardeo continuo de anuncios emergentes en la pantalla. Anuncios molestos y que son difícil de cerrar.
- Se instalan nuevas barras de herramienta que ofrecen iconos o enlaces hacia otras webs que no hemos indicado.
- Aunque no es lo más habitual, pero en ocasiones este tipo de ataques también puede hacer que nuestro equipo funcione de una forma más lenta, hasta tal punto que cualquier acción habitual puede tardar varios minutos en completarse.

Ejemplos de secuestradores de navegadores

A continuación veremos algunos de los secuestradores más peligrosos, explicando algunas de sus características y los programas que podemos utilizar para acabar con ellos (en acens no nos responsabilizamos de las modificaciones que hagan estos programas en tu equipo).

a) Qvo6

Se trata de un secuestrador de navegador que cambia la configuración de los navegadores más populares como Mozilla Firefox, Internet Explorer o Google Chrome entre otros. Una vez que ha infectado el equipo, se convierte en la página de inicio, obligando a utilizar su motor de búsqueda, un motor que ofrece las opciones habituales que cualquier otro motor de búsqueda, con la salvedad de que al realizar la búsqueda nos abre una nueva ventana con los resultados de Google.



Una vez infectado el equipo, Qvo6 empezará a rastrear nuestros movimientos en Internet para redirigirnos a sitios web que no son de nuestro interés o que contienen otro tipo de malware, además de abrir molestas ventanas con publicidad que no nos dejará trabajar de forma tranquila.

Podemos eliminar este atacante de dos formas.

1.- Desinstalarlo desde el panel de control

Lo primero que deberíamos hacer es eliminar el programa desde la lista de “Agregar/Quitar programas”. Para esto, haz clic en el botón de "Inicio" y luego “Panel de Control -> Agregar/Quitar Programas”. Aquí deberías ver todo lo relacionado con Qvo6.com, y sólo tendrías que clicar en “Desinstalar”.

Después también sería recomendable abrir cada navegador y ejecutar las siguientes tareas.

1.1. Internet Explorer: ve a “Herramientas” -> Administrar Complementos -> Toolbars y extensiones. Aquí verás Qvo6, haz clic en “Desinstalar”. Abre de nuevo el navegador y pulsa en “Herramientas” -> Opciones de Internet -> Pestaña general. Inserta Google u otra dirección para hacerla como página de inicio por defecto.

1.2. **Mozilla Firefox**: ve a “Herramientas” -> Add-ons -> Extensiones. Busca Qvo6 y haz clic en “Desinstalar”. Ahora ve a “Herramientas” -> Opciones -> General -> Inicio. Ahora selecciona “Mostrar página en blanco” cuando Firefox se inicie o coloca alguna página web.

1.3. **Google Chrome**: selecciona “Herramientas” -> Extensiones. Aquí busca la extensión de Qvo6.com y deshazte de ella haciendo clic en la papelera de reciclaje.

2.- Mediante AdwCleaner de Xplode

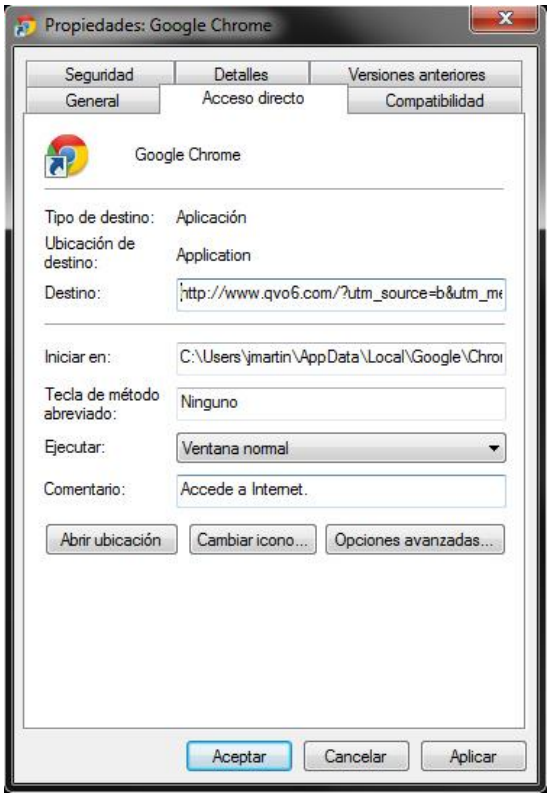
Se trata de una herramienta que permite eliminar del sistema este tipo de amenazas. Una vez instalado, nos aparecerán dos botones. El primero de ellos es el de “Búsqueda”, que analizará todo nuestro equipo en busca de alguna amenaza. El segundo botón es “Supresión”, que tendremos que pulsar en caso de que la búsqueda nos haya reportado algún tipo de amenaza.

Además de Qvo6, esta herramienta permite la eliminación de otras variantes de secuestradores como specialsavings.com o wcscriptpage.net.

3.- Eliminación en propiedades de Chrome

En ocasiones secuestradores como Qvo6 añaden una línea de código en las propiedades del explorador, de manera que cada vez que accedemos a nuestro navegador se abre una pestaña extra. Para eliminar ese código, hacemos clic derecho sobre el icono del navegador, accedemos a Propiedades-> “Acceso directo”, y en el apartado “Destino” encontraremos, después de la ruta de Chrome (C:\Users\usuario\AppData\Local\Google\Chrome\Application\chrome.exe), el código que tendremos que borrar y que será similar a:

http://www.qvo6.com/?utm_source=b&utm_medium=amt&from=amt&uid=WDCXWD800JD-75MSA3_WD-WMAM9ER7664476644&ts=1364531021



b) Specialsavings.com

Se trata de un secuestrador del navegador que una vez dentro del sistema empieza a realizar ciertas actividades maliciosas, como la modificación de la configuración del navegador o ralentizar drásticamente el sistema.

Entre las acciones que puede realizar este Hijacker están:

- Consumir toda la memoria de la CPU.
- Cambios en la configuración del navegador.
- Redirigir resultados a páginas web comprometidas, mostrando un elevado número de publicidad de poco interés para el usuario.
- Se conecta a servidores para realizar la descarga de otro tipo de malware.
- Problemas de conexión a Internet.
- Mensajes de errores y alertas.

Como en el caso visto anteriormente, a la hora de proceder a su eliminación podemos actuar de dos formas. Una manual donde eliminamos toda referencia a este programa, de forma similar a los pasos vistos en el caso de Qvo6. La otra opción es de forma automática, por medio de algún software antimalware como puede ser SpyHunter o alguno similar.

c) Scriptpage.net

Se trata de un programa capaz de no sólo modificar la configuración del navegador, sino también de cambiar los valores de los registros del sistema, haciendo que el funcionamiento de éste no sea el adecuado.

Algunos de los síntomas más comunes de este malware son:

- Empiezas a recibir gran cantidad de correo basura.
- Cualquier búsqueda te lleva a una página web desconocida.
- No te permite acceder a portales relacionados con la seguridad informática.
- Desaparición de ciertas funciones en el sistema como la administración de tareas.
- Velocidad de navegación muy lenta.

La forma de acabar con este tipo de amenaza es similar a la que hemos visto en los puntos anteriores.

Otros tipos de hijacking

Aunque a lo largo de este White Paper estamos hablando de secuestradores del navegador, también nos podemos encontrar otro tipo de secuestros en el mundo de la informática.

- **IP hijakers**: Se trata de un secuestro de una conexión TCP/IP permitiendo a un atacante inyectar comandos o la realización de un ataque DoS.
- **Page hijakers**: En este caso hace referencia al secuestro de una web, permitiendo al usuario realizar cambios en el site por medio de algún fallo de seguridad en la programación o bien en el servidor.
- **Session hijacking**: se refiere a la posibilidad de duplicar las credenciales de autorización en una comunicación válida ya establecida entre un server y un cliente (también llamada 'session') para obtener el acceso a la información o s los servicios en el servidor.
- **Domain hijacking**: Este tipo de acciones se da cuando se cambian los datos del titular de un dominio sin el consentimiento del actual titular del mismo, lo que puede llevar a la pérdida del control del mismo.

Para poder evitar este tipo de situaciones el altamente recomendable instalar un programa que proteja nuestro equipo ante cambios inesperados, o cambios no iniciados por el usuario. **Tener instalado un buen antivirus y mantenerlo actualizado**, así como tener un firewall activado, y las actualizaciones correspondientes del sistema operativo utilizado, nos ayudará a evitar no solo la infección de hijackers, si no de virus, gusanos, troyanos, hackers, crackers y otras amenazas de Internet.