# Web *Dialer* o Internet *Dumping*: ¿cómo protegernos?

**Por Ing. Yuselis Ortiz Hernández**
**Especialista Gerencia Antifraude, ETECSA**
**yuselis@etecsa.cu**

## Introducción

Con el desarrollo y la aceptación rápida y masiva de Internet a nivel mundial, han surgido nuevas facilidades para los usuarios. La red ha logrado llegar a un número de clientes inimaginable en sus inicios, a tal punto que ha ocupado el lugar de las redes de datos tradicionales y ha llegado a ser el modelo de red pública de datos.

Esta evolución unida a la utilización creciente del comercio electrónico, la falta de conocimientos sobre la seguridad de la información por parte de los usuarios, la ausencia de herramientas legales, y sobre todo a las vulnerabilidades existentes en la tecnología, traen consigo el desarrollo de elementos negativos que afectan directamente la confidencialidad, integridad y disponibilidad de la información. Formando un conjunto de condiciones propicias para que se incrementen de forma significativa los riesgos a la seguridad de la información [1].

Las vulnerabilidades en la tecnología, elemento definitorio en este tema, van en incremento en correspondencia con el desarrollo de la misma. Las siguientes gráficas muestran el aumento de las vulnerabilidades reportadas anualmente según la CERT/CC a partir de 1995 hasta el año 2004 [1]:

| 1995-1999 | | | | | |
|---|---|---|---|---|---|
| Año | 1995 | 1996 | 1997 | 1998 | 1999 |
| Vulnerabilidades | 171 | 345 | 311 | 262 | 417 |

| 2000-2004 | | | | | |
|---|---|---|---|---|---|
| Año | 2000 | 2001 | 2002 | 2003 | 2004 |
| Vulnerabilidades | 1,090 | 2,437 | 4,129 | 3,784 | 3,780 |

**Tabla 1 Estadísticas del aumento de las vulnerabilidades (1995-2004)**
**Fuente: Baluja García, Walter (Ver Referencias bibliográficas)**

Dentro de las causas que han provocado dicho incremento se encuentran [1]:

- Las características de operación de la red, en la cual la mayoría de los servicios descansan en modelos cliente servidor, y los sistemas de permisos y accesos son un poco complejos. Además de las ventajas que brindan a los usuarios los accesos anónimos.
- La existencia de sistemas propietarios y, por supuesto, la dependencia de los mismos, lo cual provoca que los expertos en seguridad no puedan examinar las tecnologías propietarias. Por otro lado, se incrementa la funcionalidad de la tecnología de información, pero se expone la seguridad de los sistemas. Como ejemplo de esto se tienen los controles Active X, VBScript de Microsoft, Java Script de Netscape, entre otros.

◆ Los recursos tecnológicos, digamos herramientas e información se encuentran generalmente gratis.

◆ La naturaleza humana, lo cual puede considerarse el factor más influyente, puesto que de ello depende el grado de seguridad con que se enfrenten las vulnerabilidades y riesgos existentes. Usualmente las personas dejan el tema de la seguridad a los expertos, desconociendo los riesgos y vulnerabilidades de seguridad a los que deben enfrentarse, lo cual impide su protección. En otros casos muchas entidades no realizan salvas de la información o no se posee un plan para enfrentar las contingencias. De ahí, que se puede afirmar que la carencia de educación, en cuanto a la seguridad de la información, es el aspecto que requiere mayor urgencia.

En este escenario surgen los ataques a los recursos y servicios de datos de los clientes y empresas. Los usuarios pueden ser victimas de ataques pasivos, en los cuales se monitorea o escucha su comunicación. Pero también pueden ser victimas de ataques activos, los cuales provocan un cambio en el flujo de datos o la creación de uno falso. Los motivos de los atacantes son disímiles: monetario, el acceso a recursos limitados, competencia, conflictos personales, entre otros.

Al principio, los virus informáticos constituían la principal amenaza para las redes de datos. Con posterioridad aparecieron un conjunto de programas malignos, los cuales han sido evaluados teniendo en cuenta los daños que causan, la rapidez de su distribución así como el salvajismo con que atacan los recursos de sus víctimas. Dentro de ellos cabe mencionar a los gusanos, Caballos de Troya, Bombas lógicas, Puertas traseras, Jokes y Hoaxes.

En la actualidad como los vendedores y empresas se han adaptado al ambiente cambiante de las amenazas a través de la implementación de buenas prácticas y estrategias de seguridad y defensa, los atacantes han adoptado nuevas técnicas. Esto ha dado como resultado que el principal objetivo de los ataques y códigos maliciosos sean las aplicaciones del lado del cliente, tales como los navegadores Web, clientes de correo, entre otros. Estas aplicaciones son usadas para comunicarse sobre redes e interactuar con servicios y aplicaciones Web. También se pueden incluir programas como procesadores de palabras, o programas *spreadsheet,* los cuales pueden abrir contenido no confiable descargado o recibido por un cliente en la red. [2]

Así, a pesar de los ya conocidos que forman parte de las amenazas definidas, cabe incluir dentro de los riesgos de seguridad a los *Dialers*, *Spyware*, *Adware,* Correos *Spam, Keyloggers*, entre muchos otros.

◆ **Dialer —marcador automático—**: es un programa que crea una conexión a Internet o a otra red de computadoras a través de un teléfono conectado a un módem o una red RDSI —Red Digital de Servicios Integrados—. Su objetivo es cortar la conexión telefónica que se está utilizando en ese momento —que permite el acceso a Internet marcando un determinado número telefónico— y establecer otra marcando un número telefónico de tarificación adicional, conocidos como números PRS —*Premium Rate Service*— y NTA —Números de Tarificación Adicional—.

◆ *Spyware*: suelen ser programas gratis que incluyen un programa pequeño o código que logran subir a una página Web o correo electrónico para recopilar información sobre una persona u organización. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirla a empresas publicitarias u otras organizaciones interesadas. También se han empleado en círculos legales para compilar información contra sospechosos de delitos. Permiten hacer perfiles de clientes, y así personalizan el envío de mensajes promocionales.

◆ **Adware**: software que durante su funcionamiento despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes o a través de una barra que aparece en la pantalla.

◆ **Spam**: correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es una forma extremadamente eficiente y barata de comercializar cualquier producto. La mayoría de los usuarios están expuestos a este correo basura que se confirma en encuestas que más del 50 % de todos los mensajes son correos basura. No es una amenaza directa, pero la cantidad de ellos generados, y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet [3]. Además constituye una fuente muy importante para la propagación de marcadores automáticos, virus, troyanos, y otros programas maliciosos.

◆ **KeyLoggers**: programa que intercepta todas las pulsaciones realizadas en el teclado de la computadora donde esté instalado, y las guarda en un archivo para obtener datos sensibles como contraseñas, etc. Posteriormente puede ser enviado a un tercero sin conocimiento ni consentimiento del usuario, a través de correo electrónico o subirlo a un servidor FTP, para que otros puedan analizar lo que el usuario escribió en su teclado [4].

Como ya se mencionó, una de las nuevas amenazas surgidas son los Marcadores Automáticos. A los cuales se ha decidido dedicar este espacio debido a las grandes afectaciones económicas y de servicios que está provocando a las empresas

de telecomunicaciones del mundo y en Cuba. Actualmente los marcadores automáticos maliciosos son tema de discusión en foros anuales y conferencias de organizaciones internacionales dedicados a la lucha contra el fraude. Tal es el caso de FIINA —*Forum International for Irregular Network Access*/Fórum Internacional para el Acceso Irregular a las Redes de Telecomunicaciones—.

## ¿Cómo surgen los marcadores automáticos?

Los marcadores automáticos aparecen con el surgimiento de contenidos especiales ofertados telefónicamente, tales como: líneas calientes, consultas financieras, apuestas deportivas, etc. Las empresas dedicadas a proveer este tipo de servicios contratan al operador de telecomunicaciones de su país varios números telefónicos. Estos números son conocidos como NTA —Número de Tarificación Adicional— ó PRS —*Premium Rate Service*— la tarifa de llamadas hacia ellos será superior a la normal debido al servicio adicional que se brinda a través de los mismos, por lo tanto estas **pequeñas** empresas reciben una parte del costo de la llamada que se le factura al usuario final.

Este es un tipo de servicio que ofrecen los operadores de telecomunicaciones —no en Cuba— a determinados clientes dueños de pequeñas/medianas empresas. Las empresas pueden ser hospitales, bancos, empresas privadas que brindan consultas de horóscopos, pornografía, líneas calientes, deportes, finanzas, y otros. Sin embargo, también se utiliza como mecanismo de fraude, al no dar advertencia alguna y aprovecharse de usuarios con conocimientos limitados sobre el tema. Uno de los más habituales, en un principio, consiste en llamar a un teléfono particular, localizado al azar en la guía telefónica, y decir al titular de la línea que ha ganado un premio y que para recibirlo debe llamar a un número —de tarificación adicional—, o alguna historia similar. Cuando el usuario llama se le tiene a la espera o se le da largas indefinidamente [5].

En la actualidad, con la evolución y aceptación de Internet, también migraron hacia este ambiente dichos servicios especiales. A los cuáles se accede a través de una conexión de datos a servidores Web con contenidos de gran demanda y que tienen asociado un número telefónico para la conexión y descarga de la información requerida. Recientemente se ha incluido la descarga de melodías gratis para móviles, música o de programas gratuitos. En este caso del acceso a los contenidos especiales a través de una conexión de datos, es habitual el uso de programas de marcado telefónico automático que establecen una conexión de acceso telefónico a redes mediante un NTA. Es decir, el usuario final paga el acceso a estos contenidos especiales a partir de su factura telefónica.

Hasta este punto dicha forma de pago es legal, siempre y cuando se advierta al usuario sobre los gastos en que incurrirá si acepta acceder a estos contenidos. Pero también en este entorno son utilizados para cometer fraude, el mecanismo más empleado en estos tiempos para generar llamadas fantasmas hacia estos números es a través de los mencionados Web *Dialers* que obligan a los clientes sin su consentimiento a hacer llamadas internacionales de larga duración.

¿La ganancia? La empresa que brinda los servicios de alta demanda mantiene una tarifa plana por una cantidad de minutos de tráfico fijo con el proveedor de servicios de telecomunicaciones. Consecuentemente, a medida que aumenta el tráfico hacia los NTA, las ganancias para ambos aumentan. Es entonces cuando aparecen las trampas para buscar mecanismos que aumenten la cantidad de llamadas y la duración de las mismas hacia los NTA.

En nuestro país las afectaciones económicas provocadas por este hecho ascienden a miles de CUC. Aunque nuestra empresa ETECSA no brinda contratos de NTAs, nuestros clientes son afectados por números que pertenecen a otros países del mundo. La principal afectación, en nuestro caso, se presenta a los clientes residenciales con salida internacional y conexión conmutada a Internet —los que en su mayoría no tienen ingresos económicos altos—, a los cuales una vez afectados por el *Dialer* malicioso le son facturadas llamadas internacionales en extremo costosas y con un promedio de duración de 40 minutos aproximadamente. Por lo tanto, además del tema económico se crea un problema muy difícil al proveedor de servicios para con sus clientes, los cuales no comprenden el incremento inexplicable de sus facturas telefónicas además del hecho de ser responsables de las mismas.

## ¿Cómo se instalan los *Dialers*?

Esta modalidad se denomina Internet Dumping o Módem Hijacking y ocurre cuando la conexión telefónica que mantiene conectada la computadora del cliente con su proveedor de servicios de Internet, es cambiada y reconectada a otro número telefónico sin el total conocimiento o consentimiento del cliente [6].

El nuevo número, generalmente, es internacional y cuenta con una tarificación adicional superior a la normal, las cifras que muestran las víctimas han ido incrementándose de forma alarmante a nivel mundial.

Algunos *Dialers* se ejecutan automáticamente cuando se enciende la computadora, estableciendo por sí solos una conexión conmutada. Y estarán en red todo el tiempo que esta permanezca encendida y esté conectado el módem a la línea tele-

fónica. Hay otros que esperan hasta que la máquina se encuentre desocupada para hacer el marcado automático o, incluso, son configurados de manera que la encienden automáticamente y realizan el marcado en horarios en que el usuario supuestamente está durmiendo y no detectará que su computadora está encendida. Los *Dialers* pueden ser enviados también vía correo electrónico y no son reconocidos fácilmente [6].

Los marcadores automáticos maliciosos frecuentemente están vinculados a sitios pornográficos o a sitios con material pirata —juegos, música, programas gratis, descarga de tonos para móviles, horóscopos, consultas de deportes, entre otros—.

Estos programas afectan únicamente a los usuarios que acceden a Internet mediante RTB —Red Telefónica Básica— ó RDSI, además a los clientes con teléfonos móviles que cuentan con la facilidad de acceso a Internet. También podrían afectar a usuarios de cable ó ADSL —*Asymetrical Digital Subscriber Line*— que tengan un módem convencional de respaldo.

Actualmente los proveedores del servicio de tarificación adicional deben informar claramente al usuario, previo su acceso a los contenidos, acerca del precio máximo por minuto, de las características del servicio, de la identidad del prestador, del procedimiento para dar fin a la comunicación y de la página Web desde la que se puede descargar gratuitamente un programa que impida la instalación de *Dialers* no solicitados.

Desafortunadamente, en la mayoría de los casos de *Dialers* **malos** esto no ocurre, y en pocos sitios se le informa al cliente a través de ventanas de texto con la letra muy pequeña o en otro idioma. Este último caso evita que el cliente esté consciente de las consecuencias y, además, se salvan responsabilidades. Por lo tanto, es una obligación de los usuarios estar atentos a todos los indicios e instalar las herramientas de seguridad imprescindibles para su protección.

## Conclusiones

La modalidad de fraude de Internet Dumping o Modem Hijacking realizada a través de los marcadores automáticos ha afectado a millares de clientes en el mundo, conectados a Internet a través de enlaces conmutados, líneas RDSI ó teléfonos móviles. Los proveedores de servicios buscan medidas alternativas para proteger a sus clientes, aunque los internautas son los responsables de la seguridad en su terminal, teniendo en cuenta que los números de los servicios NTA varían con rapidez y los defraudadores buscan vías para aprovecharse de las vulnerabilidades de los sistemas.

ETECSA como proveedor de servicios puede disminuir la afectación a sus clientes a través del monitoreo de los números internacionales conocidos como *Dialers*, y entablando reclamaciones a otros proveedores de servicio internacionales a los cuáles pertenecen dichos números. Aún así, si los clientes no protegen sus terminales de datos continuarían siendo afectados por el surgimiento constante de nuevos números. Por lo tanto, es importante el uso del candado electrónico durante la navegación, elemento que evitaría las llamadas internacionales aún si la computadora del usuario estuviera afectada por un *Dialer* malicioso. Otro método de protección recomendado es la actualización y activación de sistemas antivirus; pero, su uso depende en gran medida del propio cliente. De ahí la importancia de educar a los clientes como principal arma de protección ante esta amenaza. El usuario debe tener, además, conocimiento del problema y responsabilidad total sobre la seguridad en su terminal de datos para lograr que esté alerta durante la navegación.

## Recomendaciones

Se proponen a continuación un grupo de medidas para los usuarios con acceso conmutado a Internet [7,8]:

1.Protección mediante Software, usar herramientas de seguridad para proteger el terminal de datos (PC), asegurarse de tener actualizadas las herramientas de protección una vez instaladas. Existen programas que resultan muy eficientes para la detección de los *Dialers*, así como de cualquiera de las amenazas a las que se exponen los usuarios durante la conexión a Internet, por ejemplo los cortafuegos, Anti-Virus, Anti-Spyware, Anti-*Dialers*.

2.Durante la navegación evitar la entrada a vínculos desconocidos o a sitios que ofrezcan acceso gratuito. En caso de hacerlo, debe permanecer atento a los posibles indicios de la presencia de *Dialers*.

3.Las definiciones de seguridad en el Internet Explorer deben incrementarse. Algunos *Dialers* se instalan automáticamente aprovechándose de los *scripts* de las páginas Web. Desactivar —en caso de usar Internet Explorer— ActiveX en el navegador pues son componentes utilizados por muchos sitios Web para instalar *Dialers* automáticamente.

4.La computadora debe estar apagada o desconectada la línea telefónica del módem cuando no esté en uso o cuando el usuario no vaya a estar en la casa.

5.No conectarse a Internet a través de una línea con marcación internacional directa. En caso de no utilizarse este servicio, solicitar al operador su desconexión.

6.Actualización del sistema operativo.

7.La contraseña de la conexión conmutada no debe estar almacenada en el equipo. Es mejor si el usuario ingresa dicha información en cada nueva sesión, lo cual es importante porque algunos *Dialers* registran los NTA que tienen configurados en sí mismos como la conexión regular del usuario. Y al mantener la contraseña en la máquina el usuario no verifica la numeración para la conexión.

8.Los usuarios deben cerciorarse de que el sonido del módem se escuche cuando se produzca el marcado. Esta no es la mejor forma de protección, pues algunos *Dialers* desactivan el sonido del módem antes de efectuar el marcado. No debe silenciarse la bocina.

9.Windows Messenger es práctico, sobre todo, si se desea enviar mensajes instantáneos dentro de una red, pero también puede ser usado inadecuadamente para bombardear a desconocidos con pulicidad no deseada. En ese caso, se recomienda cerrarlo.

10.Si se accede a una oferta que tiene prerequisitos como aceptar un certificado de seguridad o si se le solicita escribir algo, el usuario debe actuar con precaución.

11.Debe prestarse atención a símbolos desconocidos en la barra de tareas o en el escritorio durante la navegación.

12.La lista de conexiones conmutadas hay que verificarla frecuentemente en busca de entradas nuevas o desconocidas.

13.Debe verificarse la carpeta **Archivos de programas descargados**, pues muchos *Dialers* utilizan esta carpeta, la cual se encuentra dentro del directorio Windows —comúnmente C:\Windows—, para colocar sus controles ActiveX. Estos pueden causar una descarga automática o una conexión de marcado de un *Dialer* si visita una página Web específica.

Existen preguntas muy frecuentes que suelen hacer los usuarios, entre las cuales se encuentran:

**¿Cómo este programa aparece en la computadora?**

Se descarga automáticamente desde una página Web con contenidos especiales o como adjunto de un correo electrónico descargado por el usuario.

**¿A dónde llamará la computadora?**

El módem marcará el número que tiene configurado el *Dialer* que se ha descargado en la PC —este número puede ser internacional—. El precio de la llamada dependerá del lugar de destino —los destinos hacia los que han sido efectuadas la mayor cantidad de llamadas de clientes afectados en Cuba han sido: Reino Unido, Samoa, Holanda, San Marino, Emiratos Árabes, Sao Tomé de Príncipe, Austria, Bélgica, Guinea, entre muchos otros—.

**Si no había nadie en casa ¿cómo se pudieron realizar estas llamadas?**

Una vez que el *Dialer* reside en la computadora, algunos cuentan con un temporizador, a través del cual se define el tiempo que rige la sistematicidad con que serán efectuadas las llamadas. En este caso la marcación puede ocurrir varias horas o días después del usuario haber terminado la conexión a Internet o haber descargado el *Dialer* —siempre y cuando la computadora y el módem estén encendidos y este último se mantenga conectado a la línea telefónica—.

## Referencias bibliográficas


[1] Baluja García, Walter. Postgrado de Cifrado y Seguridad en Redes, Departamento de Telemática. La Habana: CUJAE, 2005.

[2] Informe de Amenaza de Seguridad en Internet de Symantec (marzo/2006). Disponible en: http://www.acis.org.co/fileadmin/Resumen_Ejecutivo.doc. (Consulta: marzo/2006)

[3] Centro de alerta temprana sobre virus seguridad informática. Disponible en: http://alerta-antivirus.red.es/seguridad/ver_pag.html?tema=S&articulo=9&letra=C. (Consulta: marzo/2006)

[4] Virus Atack. Disponible en: http://virusattack.virusattack.com.ar/articulos/VerArticulo.php3?idarticulo=57(Consulta: marzo/2006)

[5] Anti-Dialers. Disponible en: http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=7. (Consulta: enero/2006)

[6] Internet Dialers. Manchester News Technology. Disponibble en: http://www.manchesteronline.co.uk/news/technology/s/132/132647_action_on_rogue_internet_diallers_.html (Consulta: agosto/2005)

[7] FIINA. Forum International for Irregular Network Access (Conferencias octubre/2005, Noviembre/2006).

[8] Internet Diallers. Telstra Library. Disponible en: http://www2.telstraclear.co.nz/online-tools/library/Diallers/#diallers. (Consulta: junio/2005)

[9 Premium Rate Dialers Scams. Internet Watch Foundation. Disponible en: http://www.iwf.org.uk/howto/page.20.238.htm. (Consulta: junio/2005)


### Sitios útiles para los usuarios

http://alerta-antivirus.red.es/utiles/ver.php?tema=U&articulo=7&pagina=0
http://www.2-spyware.com/remove-trojan-win32-Dialler-af.html
http://www.e-mexico.gob.mx/wb2/eMex/eMex_Virus_Noticias
http://www.noticiasdot.com/publicaciones/2003/1003/0110/noticias011003/noticias011003-4.htm
http://www.pandasoftware.es/virus_info/faq.asp
http://www.pandasoftware.es/virus_info/glosario/
http://www.stopdial.com
http://www.vsantivirus.com/dialler-af.htm
http://www.worldslargestnetwork.com/Identifying-Malicious-Diallers.html

## Glosario

**Virus**: programas que se reproducen infectando otros archivos o aplicaciones; realizan acciones perjudiciales para el usuario.

**Gusanos**: programas que no necesitan infectar otros archivos para reproducirse, y se propagan realizando copias de sí mismos, con el fin de colapsar las redes en las que se infiltran.

**Caballo de Troya**: programa aparentemente útil que funciona con el paradigma cliente/servidor, contiene funciones escondidas que emplean los privilegios del usuario que lo ejecuta. Se caracteriza por la no autopropagación y se introducen en los programas más empleados por los usuarios.

**Bomba Lógica**: son casos particulares de Caballos de Troya que permanecen inactivos mientras no se cumplan ciertas condiciones en la PC. Estas condiciones pueden ser una fecha determinada, paso de un período de tiempo, números de acceso a disco, combinación de teclas, entre otros.

**ActiveX**: conjunto de normas que definen los procedimientos de manipulación de objetos multimedia. Para cada tipo de archivo u objeto se crea un control que puede asociarse a un programa y funcionar en conjunto con él. Son componentes adicionales que pueden incorporarse a las páginas Web, para dotar las de mayores funcionalidades —animaciones, video, navegación tridimensional, etc.—.

**Firewalls**: combinación de hardware y software diseñado para examinar todo el tráfico que lo atraviesa. Su propósito es eliminar la paquetería que desentone con la política del sitio materializada en los criterios de filtrado. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, incluyen *host* bastión con servicios de *proxy* y otros.

**Jokes o virus broma**: son aplicaciones malignas que crean mensajes de broma en la pantalla. También pueden ejecutar el lector de CD/DVD abriéndolo y cerrándolo, o controlar el propio ratón, incluso, el teclado, siempre con un fin de diversión y nunca de destrucción o daño para el contenido del ordenador aunque a veces pueden llegar a ser molestos.

**Hoaxes o falsos virus**: son mensajes con una información falsa, normalmente son difundidos mediante el correo electrónico, a veces para crear confusión entre las personas que los reciben o pueden tener una finalidad más delicada, por ejemplo, perjudicar a alguien o atacar al ordenador a través ingeniería social, mensajes como "borre este archivo del equipo es un virus muy potente" y, paradójicamente, pueden ser archivos del sistema, necesarios para el arranque u otras partes importante.