

Programas de marcado no autorizados: Del problema a la solución

Introducción al problema: Los principios de su funcionamiento

Hace algunos años, apareció un tipo especial de aplicación maliciosa, denominada *Rogue Dialer* o *Trojan Dialer*: un programa de marcado telefónico deshonesto e indeseado.

Este tipo de aplicaciones, intenta realizar llamadas de larga distancia o a números específicos, que tienen un coste de conexión adicional por minuto.

Para cumplir con su objetivo, el ordenador de la víctima debe estar equipado con un módem conectado a la línea telefónica.

Vale la pena mencionar que hay dos clases de programas de marcado:

- **Con autorización del usuario**

La primera, que es bastante legítima, agrupa las aplicaciones diseñadas para cobrar una suma de dinero a los usuarios, para acceder a ciertos sitios de Internet o a secciones restringidas.

Estos programas, ofrecen cándidamente la descarga de aplicaciones que permitirán la entrada a páginas con un interés particular (generalmente pornografía o contenido similar para adultos), y solo se instalarán en el ordenador si el usuario lo autoriza explícitamente.

- **Sin autorización del usuario**

A diferencia de la anterior, la segunda clase es completamente ilegal.

Estos programas se denominan usualmente programas de marcado engañosos (*rogue dialers*), y se instalan automáticamente, sin el conocimiento del usuario, aprovechando las vulnerabilidades de las aplicaciones u otras falencias en la configuración del sistema.

El programa de marcado podría presentar una aparente solicitud del consentimiento del usuario antes de instalarse, pero ignora la respuesta obtenida, y se instala silenciosamente en segundo plano.

Los objetivos de este tipo de aplicaciones pueden variar, desde una simple broma de advertencia, hasta la ganancia financiera, en instancias más severas.

Para que esto suceda, un perpetrador necesita registrarse y configurar un número telefónico especial.

Muchas compañías telefónicas ofrecen un servicio a tasa preferencial optativo para sus clientes, que les permite organizar encuestas por votación sobre la televisión y proporcionar otro tipo de servicios comerciales.

Al desarrollar o solicitar el programa de marcado para el número de teléfono asociado, el delincuente puede ganar dinero real.

Veamos ahora un esquema típico para organizar un negocio en base al marcado telefónico.

Este esquema se aplica tanto a los programas legales como ilegales:

- **La compañía principal** (similar a un proveedor de Internet) arrienda la línea telefónica y crea un número especial para módem, con un equipamiento capaz de cobrar cierta suma de dinero por acceder a él. Estas compañías desarrollan versiones únicas de programas de marcado, y las complementan con un equipo de rastreo de números para derivar los pagos.
- **Los clientes son empresas** que proporcionan acceso pago a sus recursos. Utilizan los servicios que brindan las compañías principales.
- **Los sitios intermediarios** son sitios de Internet, que ponen publicidad y enlaces a los programas de marcado en sus páginas. Estas últimas, también podrían alojar códigos que aprovechan vulnerabilidades de los sistemas, como guiones que se ejecutan en segundo plano e instalan marcadores inadvertidamente. Cada sitio de este tipo tiene un número de identificación suplementario además del número de suscriptor principal, para ayudar al rastreo y la cuenta de los accesos.

Cuando alguien realiza una llamada, el equipo en la compañía principal recibe su número de identificación, con el fin de cobrarle la suma de dinero correspondiente.

El usuario es redirigido a las áreas restringidas que mantienen los clientes individuales.

El resultado es que la compañía y sus clientes obtienen su porción de ganancias, mientras que el inocente usuario sufre el impacto del coste del acceso a este tipo de líneas.

El daño sufrido por las operaciones de marcado puede ser significativo.

El autor conoce experiencias en las que el acceso a líneas especiales tuvo costes que varían entre 75 y 750 euros, y estos casos son bastante comunes.

De acuerdo a informes no confirmados, hay denuncias en las que los daños ascienden a los 2300 euros.

Si tenemos en cuenta que la tarifa de conexión promedio oscila entre 1,50 y 3,90 euros (en algunos casos, puede llegar a los 7,70 euros por llamada), la suma de los daños ocasionados puede resultar sorprendente.

A menudo, las víctimas de este tipo de ardides, intentan apelar contra los costes cobrados, asegurando que fueron víctimas y no se debería efectivizar ese pago.

En estos casos, la compañía telefónica examina los registros realizados por el equipo de facturación para comprobar la conexión, habilitando al operador a proceder con la solicitud de pago.

No se ha registrado un solo caso en el que el usuario afectado no haya tenido que abonar el monto completo.

Esto significa que las personas que hicieron las llamadas, finalmente tuvieron que pagar por ellas.

Las compañías de telecomunicaciones y otras organizaciones, incluyendo las presiones legales, no pueden acusar a los autores de los programas de marcado, porque los desarrolladores de aplicaciones legales están protegidos por el consentimiento formal del usuario al instalarlas.

Los autores de marcadores ilegales, utilizan servicios de estados extranjeros, que no tienen leyes específicas contra este tipo de actividades.

Además, las sumas de dinero que obtienen dichos estados puede ser sustancial, hecho que los desalienta a obstruir estas operaciones.

A pesar de que el acceso a Internet a través de banda ancha ha reemplazado al antiguo marcado telefónico en muchas regiones, el problema con los marcadores ilegales todavía persiste. Esto se debe a varios factores:

- Muchos ordenadores todavía tienen módems integrados conectados a la línea telefónica. Aún si el usuario no se conecta a Internet a través de ese módem, el marcado automático puede producirse inadvertidamente mientras el módem está activado.
- Desconectar el módem no es una solución, porque algunas personas los utilizan para enviar y recibir faxes.
- Pero, el factor predominante del uso de los marcadores telefónicos, es el desarrollo inadecuado de los servicios de banda ancha en áreas como Asia, Europa Oriental, Sudamérica, África y otras regiones tecnológicamente limitadas.

Debido a las razones expuestas, el acceso telefónico todavía es un medio para estar en línea, popular y extendido, por lo tanto es importante proteger a los usuarios contra los programas de marcado engañosos.

Causas e indicios de la instalación de un marcador

Los programas de marcado pueden infiltrarse en un ordenador de varias maneras, pero el típico escenario de infestación sería similar al siguiente:

- Mientras navega por un sitio de Internet, principalmente de contenido adulto o de entretenimiento, un usuario recibe un mensaje de error que indica la imposibilidad de acceder a determinada información. El sitio solicita la descarga de un programa especial, que está diseñado para permitir el acceso, después de marcar un determinado número telefónico.

- Cuando el usuario acepta, un pequeño archivo se descarga y se instala.

Vale la pena mencionar que la mayoría de las alertas que muestra el marcador tienen una característica interesante: suelen estar en un idioma diferente al del usuario.

En casi todos los casos, este directamente no comprende el significado de los mensajes e, inadvertidamente, aprueba la instalación y el llamado subsiguiente.

El autor de este artículo ha evaluado programas de marcado que utilizaban alemán, italiano e inglés en los cuadros de diálogo.

- Después de que el marcador se instala, interrumpe la conexión actual, y marca el número especial.
- Como resultado, las secciones restringidas del sitio se vuelven disponibles.

Algunos sistemas son tan sofisticados que permiten que el usuario no solo acceda a direcciones específicas, sino que también actúa como proveedor de Internet.

Esto podría provocar que el usuario pase una cantidad de tiempo considerable, conectado a un marcador que le cobra precios exorbitantes.

Los programas de marcado también pueden trabajar clandestinamente en cualquier momento, desde la etapa de instalación hasta la llamada actual.

Una conexión puede establecerse sin el conocimiento del usuario, un programa malicioso puede detectar la conexión a Internet activa, interrumpirla y reconectarse a un número específico que después se convertirá en la conexión predeterminada.

El programa también puede modificar las propiedades de marcado actuales, reemplazando el número de acceso original por otro fraudulento, y realizar las llamadas a dicho número.

Algunas aplicaciones de marcado ilegales pueden detectar cuando el ordenador está inactivo (monitorizando la actividad del ratón y del teclado), y hacer llamados cuando el usuario supuestamente no está presente.

Lo síntomas que indican una infección por un programa de este tipo pueden ser varios, desde las modificaciones visibles de las propiedades de marcado, hasta desconexiones espontáneas del módem y la subsiguiente restauración del acceso, un descenso en la velocidad de la conexión a Internet sin razón aparente, una línea telefónica ocupada cuando aparentemente el módem no está en uso, o un sonido del módem cuando se levanta el tubo del teléfono.

Debemos aclarar que algunos expertos recomiendan activar el sonido del módem, como una precaución contra los programas de marcado indeseados, pero en algunos casos el marcador puede desactivar temporalmente el sonido y volver a encenderlo después de concretar su misión.

La respuesta de las compañías de seguridad y las deficiencias de las aplicaciones antivirus

Por muchas razones, las compañías antivirus no han respondido adecuadamente a los programas de marcado.

Algunos desarrolladores prácticamente ignoraron la existencia de este tipo de código malicioso, otros no lo detectaban ni lo consideraban en sus configuraciones predeterminadas.

Sólo una porción de las empresas de seguridad informática incluyeron las aplicaciones de marcado en sus bases de datos de amenazas conocidas, pero apenas fue suficiente: a medida que aumentaba la cantidad y la complejidad de los marcadores, las bases de datos debían ser adecuadamente actualizadas.

Los programas de marcado son, en cierta forma, aplicaciones controvertidas.

Sus desarrolladores toman activas medidas con el fin de revertir su imagen, y clasificar dichos programas no como código destructivo, sino como aplicaciones de publicidad, o programas para acceso exclusivo. Ellos alegan que el marcado formal se realiza con el consentimiento del usuario, como cuando se advierte que finalizará la conexión actual y se marcará un número diferente.

En algunas ocasiones, el precio de la llamada se menciona en las instrucciones, u otra información adjunta.

Por lo tanto, los autores de los programas de marcado demandan que los desarrolladores de antivirus, eliminen sus aplicaciones de las listas de firmas de código malicioso.

En los años 2005 y 2006 aproximadamente, las compañías antivirus comenzaron a encarar el problema de los programas de marcado no autorizado.

Junto a ellas, otros proveedores como empresas de telecomunicaciones y proveedores de servicios de Internet incluyeron algún tipo de protección contra este tipo de aplicaciones para sus usuarios.

Eso a llevado a que prácticamente cada producto antivirus incluya alguna forma de protección contra los marcadores maliciosos.

Pero, desafortunadamente, la mayoría de los desarrolladores siguieron el mismo camino al crear este tipo de protección: interceptar las funciones de llamado incluidas en librerías, como los comandos **RasDial** o **tapiRequestMakeCall**, en modo usuario.

Lamentablemente, este tipo de interceptación no puede proporcionar protección total.

Además de utilizar funciones de librerías como RAS API (Interfaz de programación de aplicaciones de servicio de acceso remoto, *Remote Access Service Application Programming Interface*) y TAPI (Interfaz de Programación de Aplicaciones vía Telefónica), un programa puede iniciar un llamado escribiendo directamente en el puerto (utilizando las funciones *CreateFile*, *WriteFile*, *CloseHandle*).

La interceptación de las funciones de librería estándar por las compañías de seguridad, no soluciona el problema, porque los procedimientos pueden ser modificados de tal modo que la aplicación antivirus no impedirá la capacidad de escribir directamente en el puerto del dispositivo.

Algunos productos contra los programas de marcado fueron un poco más lejos: agregaron un controlador especial que rastrea los datos enviados al módem, y los analiza en busca de comandos específicos de estas aplicaciones maliciosas. Con estos ajustes, se podía eludir efectivamente los intentos de marcado ilegítimos, pero un análisis más minucioso podría revelar algunas debilidades preocupantes.

La rutina de filtración incorrecta del flujo de datos podría permitir a los marcadores operar desapercibidamente bajo este tipo de soluciones de seguridad. Esto significa que los sistemas de control pueden ser evadidos mediante modificaciones específicas de los comandos.

La solución: el complemento DialStop

El autor de este documento ha realizado un análisis en profundidad de todas las vulnerabilidades existentes en los sistemas conocidos contra los programas de marcado.

Las fallas descritas en el presente informe, y la necesidad de proteger efectivamente a los usuarios de módems, ha llevado a la creación de un sistema propietario contra los marcadores no autorizados.

Se basa en un controlador en modo núcleo (por lo tanto evita las vulnerabilidades propias de la interceptación de funciones de librería estándar) unido a un algoritmo adaptable para el análisis de datos que garantiza una detección confiable y que consulta ante la presencia de un intento de conexión.

El controlador del sistema verifica la integridad y la validez de los datos transmitidos, protegiéndose contra el sabotaje causado por código malicioso y la elevación de los privilegios del sistema.

Esto se hace a través de la validación de los paquetes, y su tamaño relativamente reducido.

Si un programa malintencionado intenta reinstalar un módem en el sistema, con la intención de evadir los controles de seguridad, el complemento **DialStop** detectará el cambio y ofrecerá protección para el módem.

El sistema está diseñado para funcionar en plataformas Microsoft Windows 2000/XP/2003 Server y está [disponible sin coste alguno](#) en el sitio web de Agnitum, como complemento para Outpost Firewall Pro.

Este artículo ha sido escrito con la contribución del autor del sistema DialStop, [Oleg Bil](#).