

Procesos que pueden favorecer la fuga de información

Prólogo

De forma legítima y habitual, el sistema operativo Windows permite la modificación de procesos en curso a través de distintas técnicas válidas y legítimas, sin embargo, muchas de las mismas pueden ser utilizadas subrepticamente, por código malicioso, para actividades fraudulentas y en perjuicio del sistema atacado.

Por favor, consulte la [introducción](#) a nuestra sección Glosarios, para una mejor comprensión de los criterios, terminología y convenciones utilizadas.

Presionando el atajo de teclado **Control + F** podrá hacer búsquedas simples en esta página.

Glosario

Inyección de componentes

El sistema operativo Windows, de manera predeterminada, permite instalar interceptores de sistema (anzuelos) mediante los cuales es posible inyectar código externo en otros procesos.

Por lo general, esta técnica se utiliza para acciones comunes y legítimas, como por ejemplo, cambiar la distribución del teclado o abrir un archivo PDF dentro de la ventana del navegador de Internet.

Sin embargo, la misma puede ser utilizada, de igual forma, por programas maliciosos para insertar código dañino y así secuestrar la aplicación huésped.

Un ejemplo de este tipo de fuga es analizado, montando un ataque simulado, a través de un programa de PC Audit que puede ser descargado desde <http://www.pcinternetpatrol.com/>.

Outpost Firewall Pro controla la instalación de interceptores de anzuelos en el espacio de la dirección asignada al proceso. Esto se implementa por medio de la interceptación de funciones que son utilizadas, habitualmente, por procesos maliciosos (troyanos, programas espía, virus, gusanos, entre otros) para implantar su código en procesos legítimos (es decir, Internet Explorer o Firefox, por ejemplo).

El comportamiento de un archivo DLL que invoque tales funciones se considerará sospechoso y desencadenará una verificación legítima.

Control sobre otra aplicación

La tecnología DDE se utiliza para controlar aplicaciones.

Y de hecho, la mayoría de los navegadores más conocidos son servidores DDE y también pueden ser utilizados por programas maliciosos para transferir información privada en la red.

Un ejemplo de este tipo de fuga, podemos observarlo a través de herramientas de análisis específicas, como **Surfer**, que puede ser descargado desde <http://www.firewallleaktester.com/leaktest15.htm> y, también por la utilidad ZABypass.

Con Outpost Firewall Pro, cada intento de utilizar la intercomunicación DDE será monitorizado sin exclusiones, ya sea que el proceso se encuentre abierto o cerrado.

El control de comunicaciones entre procesos DDE permite a Outpost Firewall Pro controlar los métodos utilizados por ciertas aplicaciones para obtener control ilegítimo sobre procesos válidos.

Esto evita que el código malicioso pueda secuestrar un programa legítimo y, al verificar esta interactividad a nivel DDE, comprueba si está autorizado a ejecutarse sobre las aplicaciones habilitadas para la red.

En caso de detectarse este tipo de intento, se desencadenará una verificación legítima.

Control sobre las ventanas de las aplicaciones

Windows permite a las aplicaciones intercambiar mensajes entre las ventanas de los procesos.

Los procesos maliciosos pueden obtener control sobre las aplicaciones habilitadas para la red y enviar mensajes entre las ventanas, imitando el ingreso de datos por parte del usuario desde el teclado y/o pulsaciones del ratón.

Es posible verificar un ejemplo de la utilización de esta técnica, a través del análisis de fuga **Breakout**, que puede descargarse desde <http://www.firewallleaktester.com/leaktest16.htm>.

Aquí el punto importante es la interactividad de los programas a través del programa de aplicación de la interfaz (API) que le permite enviar mensajes (*SendMessage*), publicar los mismos (*PostMessage*) y así sucesivamente.

Esta técnica se utiliza, habitualmente, para favorecer la interactividad legítima entre procesos, pero de igual modo, pudiera utilizarse con propósitos delictivos por parte de terceros no autorizados. Outpost Firewall Pro controla estos intentos de control ilegítimo.

Modificación del escritorio activo

Durante la instalación del archivo HTML específico para el escritorio activo, los procesos maliciosos pueden transferir datos privados, hacia terceros no autorizados, en nombre del Explorador de Windows.

Es posible verificar un ejemplo de la utilización de esta técnica, a través del análisis de fuga **Breakout**, que puede descargarse desde <http://www.firewallleaktester.com/leaktest16.htm>.

Outpost Firewall Pro controla estos intentos de robo de información que pretenden engañar al cortafuegos a través de esta técnica.

Envío de consultas DNS

El servicio del cliente DNS contiene una vulnerabilidad potencial llamada Transmisión de datos DNS estructurados (*tunneling*).

El punto más importante está en que el código malicioso puede transferir y recibir cualquier información, utilizando paquetes DNS correctos, y a través de un servidor DNS configurado correctamente.

Un ejemplo de utilización de esta técnica lo encontramos en el análisis de fuga **DNSTester** (<http://www.klake.org/~jt/dnshell/>). Outpost Firewall Pro realiza una doble verificación del acceso al servicio del cliente DNS, lo que brinda un sistema más seguro.

Esta técnica permite controlar el acceso a la **API** (*Application Program Interfaz*, Programa de aplicación de la interfaz) de DNS, incluso con el servicio del cliente DNS activado, lo que beneficia a los usuarios, quienes, debido a problemas de compatibilidad, no pueden desactivar este servicio.

Esta funcionalidad permite asignar permisos a un proceso específico para utilizar el servicio del cliente DNS.

Lanzamiento oculto de aplicaciones

Procesos maliciosos pueden abrir el navegador de Internet predeterminado, con una dirección de Internet previamente configurada en una ventana oculta y de esta forma, el cortafuegos creará que se está realizando una acción legítima.

Los cortafuegos que confían en una aplicación explícita sin tener en cuenta, en primer lugar, quien la abrió en realidad y cuáles son los parámetros de conexión adicionales que se han brindado, no están en condiciones técnicas de impedir estos procedimientos ocultos, lo que implica la posibilidad de permitir la extracción de datos confidenciales de su ordenador.

Como ejemplos de utilización de esta técnica encontramos los análisis de fuga:

- **Tooleaky**
<http://www.firewallleaktester.com/leaktest2.htm>.
- **Ghost**
<http://www.firewallleaktester.com/leaktest13.htm>.

Outpost Firewall Pro observa cada programa que se inicia en un ordenador, y controla quién tiene permiso para iniciar esa aplicación con una dirección URL como objetivo y, como consecuencia, le preguntará al usuario si esa actividad deberá autorizarse para ese programa en particular.

Ejecución de aplicaciones con parámetros en la línea de comandos

Diversos cortafuegos se exponen a la vulnerabilidad que significa que un código depredador pueda abrir el navegador de Internet predeterminado conteniendo parámetros en su línea de comandos, lo que le permite sortear la protección existente al creer que la misma es una aplicación legítima la que está realizando dichas acciones.

Sin embargo, en esos parámetros de la línea de comandos puede existir información confidencial o crítica, junto con el nombre del servidor como receptor objetivo de la misma.

Un ejemplo de utilización de esta técnica lo encontramos en el análisis de fuga **Wallbreaker** (<http://www.firewallleaktester.com/leaktest11.htm>).

Outpost Firewall Pro brinda una lista restringida de procesos que están autorizados para iniciar el navegador predeterminado con parámetros en la línea de comandos, lo que permite proteger a su navegador contra manipulaciones ilegítimas.

Además del control sobre los navegadores tradicionales, esta protección sobre la apertura desde la línea de comandos se aplica a todos los programas habilitados para la red que estén presentes en la configuración.

Modificación de entradas críticas en el registro

Procesos maliciosos pueden modificar el registro para obtener acceso a la red en nombre de otra aplicación, por ejemplo, Explorador de Windows.

Un ejemplo de utilización de esta técnica lo encontramos en el análisis de fuga **Jumper** (<http://www.firewallleaktester.com/leaktest17.htm>).

Estos intentos son controlados por Outpost Firewall Pro mediante su capacidad proactiva de protección, permitiéndole elegir al usuario, si desea admitir la inserción de un objeto en un área específica del registro de Windows.

Control de aplicaciones mediante OLE

Esta es una técnica relativamente nueva, utilizada para controlar la actividad de las aplicaciones a través del mecanismo de Windows para vinculación e incrustación de objetos (OLE, *Object Linking and Embedding*), que le permite a un programa, controlar el comportamiento de otro en el ordenador.

Utilizando la técnica de intercomunicación que brinda OLE para intercambiar datos y comandos entre aplicaciones, por ejemplo, es posible controlar la actividad del navegador Internet Explorer, de forma tal que pueda enviar datos especificados por el usuario, a una ubicación remota.

Un ejemplo de utilización de esta técnica lo encontramos en el análisis de fuga **PCFlank** (<http://www.pcflank.com/PCFlankLeaktest.exe>).

Outpost Firewall Pro, al detectar una comunicación OLE le consultará al usuario si es normal para esa aplicación controlar la actividad de otro programa.

Modificación de procesos en memoria

Diversos troyanos y virus utilizan técnicas sofisticadas que les permiten alterar el código de aplicaciones de confianza que se estén ejecutando en memoria y, por consiguiente, evitar el perímetro de seguridad del sistema y realizar sus actividades maliciosas. Esto también es conocido como inyección de código o vulnerabilidad de copiado.

Como ejemplos de utilización de esta técnica encontramos los análisis de fuga:

- **Thermite**
<http://www.firewallleaktester.com/leaktest8.htm>
- **Copycat**
<http://www.firewallleaktester.com/leaktest9.htm>

Outpost Firewall Pro permite controlar las funciones que pueden utilizarse para escribir código malicioso en el espacio de direcciones de la aplicación de confianza. De esta forma, se evita que un proceso dañino pueda inyectar código en procesos legítimos.

Todo el espacio de memoria utilizado por cualquier aplicación activa en un ordenador es analizado por Outpost Firewall Pro y no solamente los de una aplicación habilitada para la red.

En caso que un código malicioso trate de modificar la memoria de otros procesos a nivel de la aplicación, Outpost Firewall Pro lo detectará y mostrará un cuadro de diálogo para que el usuario decida su habilitación..

El sistema funciona de manera proactiva, es decir, permite autorizar o denegar la modificación de memoria u otros procesos a nivel de la aplicación.

Por ejemplo, Visual Studio 2005 podría modificar la memoria, mientras que el análisis de fuga *copycat.exe* no tendría autorización para hacerlo.

Esta característica protege contra el código malicioso conocido no detectado por los proveedores de antivirus y de aplicaciones contra programas espía.

Acceso de bajo nivel a la red

Algunos controladores de red permiten un acceso directo al adaptador de red evitando la pila TCP estándar.

Estos controladores pueden ser utilizados por programas capturadores de paquetes de red, así como otras aplicaciones maliciosas, para obtener acceso de bajo nivel a la red. De este modo, pueden generar un riesgo adicional para el sistema dado que el tráfico que pasa por ellos no puede ser examinado por el cortafuegos.

Un ejemplo de utilización de esta técnica lo encontramos en el análisis de fuga **MBtest** (<http://www.firewallleaktester.com/leaktest10.htm>).

Outpost Firewall Pro permite controlar las aplicaciones que solicitan acceso a la red a través de evitar los métodos estándar.

Esta característica fortalece el nivel general de seguridad de la red evitando la pérdida de datos salientes.

El usuario es capaz de controlar los intentos de una aplicación por abrir un controlador habilitado para la red, lo que significa que sin la autorización del usuario, una aplicación no puede enviar datos ARP o IPX.