

## Desvío de procesos en modo núcleo o modo usuario: ¿Qué es mejor para el cortafuegos?



### Introducción

En los foros en línea y en diversos medios, existe un gran debate en relación a la capacidad de los cortafuegos, para prevenir el impacto de los códigos maliciosos “en estado salvaje” en la seguridad o la estabilidad del sistema.

Un grupo de pruebas de fuga recientemente publicadas, ha intensificado la controversia con respecto a cuál es la técnica que ofrece mejor protección: el desvío de procesos en modo núcleo o el desvío de procesos en modo usuario.

Este documento, es la contribución de Agnitum al debate, desde la perspectiva de una empresa líder en el desarrollo de aplicaciones cortafuegos.

Primero mencionaremos los potenciales beneficios de ambos métodos, y más adelante, explicaremos brevemente el motivo de nuestra particular elección al diseñar y desarrollar Outpost.

### Técnicas para controlar la interacción entre aplicaciones

Es frecuente que, en un ordenador personal, las aplicaciones se comuniquen entre ellas.

Esto sucede, por ejemplo, cuando abrimos un documento .PDF desde la ventana de exploración de Mi PC, pulsando dos veces sobre el archivo: el Explorador de Windows llama al programa configurado para abrir automáticamente esta clase de archivos, en un contexto apropiado.

Un cortafuegos debería ser capaz de detectar este tipo de interacción, y prevenir que un programa, secuestre un proceso y utilice ilegítimamente las credenciales de acceso de otra aplicación con fines nefastos.

Para lograrlo, es preciso que, tanto el cortafuegos, como los demás programas de defensa proactiva, utilicen un intermediario, conocido como desvío de funciones (*function hook*), para interceptar los comandos entre las aplicaciones, con el fin de monitorizar la interacción mutua.

Por lo tanto, para brindar una protección eficaz, las aplicaciones de seguridad necesitan controlar los procesos en ejecución, para verificar, por ejemplo, sus permisos de interacción, antes de habilitarlos para que realicen alguna actividad.

Para conseguirlo, el cortafuegos reemplaza cierta cantidad de llamadas a funciones internas del sistema, con sus propias funciones.

Este proceso de interceptación de funciones se denomina desvío de procesos (*hooking*).

Existen dos métodos ampliamente aceptados para interceptar funciones de programas:

1. Desvío de procesos en modo usuario (*user mode hooks*)
2. Desvío de procesos en modo núcleo (*kernel mode hooks*), por ejemplo, la interceptación de la Tabla de de descriptores de servicios del sistema (SSDT, *System Service Descriptor Table*).

El primer tipo de desvío es un método especial, para procesar actividades que son visibles a los usuarios, e implica menos privilegios de acceso que el modo núcleo.

El segundo, en cambio, es una implementación más global, que opera directamente desde el núcleo del sistema operativo Windows, y procesa comandos específicos.

En términos sencillos, podrían ser denominados “modo visible” y “modo oculto”, respectivamente.

Analicemos ahora las ventajas y desventajas de cada enfoque, desde la perspectiva de la seguridad del sistema.

A continuación, presentamos una tabla con las principales diferencias, que podrían ayudar a comprender mejor sus implicaciones.

| Criterio de comparación                          | Desvío de procesos en modo usuario   | Desvío de procesos en modo núcleo   |
|--|--|---|
| <b>Seguridad</b>                                 |  |   |
| 1) Desactivación de desvíos ( <i>unhooking</i> ) | Podría verse comprometido si los desvíos en modo usuario no están convenientemente protegidos. Cada método de interceptación en este modo requiere medidas de seguridad específicas contra el desmantelamiento de defensas.  | Podría ser comprometido cuando se utiliza la cuenta Administrador. La mayoría de los usuarios tienen, automáticamente, derechos de administrador, en la configuración de sus ordenadores.   |
| 2) Comunicación local entre procesos             | Puede advertir acerca de la comunicación entre procesos, en tiempo real. Esto previene: <ol style="list-style-type: none"> <li>1. La corrupción de aplicaciones legítimas.</li> <li>2. El compromiso de la integridad de los datos, o su pérdida, debido a la modificación de la aplicación de destino.</li> </ol> | No puede advertir en tiempo real, porque no es posible poner "en espera" la comunicación entre algunos procesos en modo núcleo, sin afectar la estabilidad del sistema.   |
| <b>Estabilidad</b>                               |  |   |
| 3) Confiabilidad de la operación                 | Buena, raramente causa errores en las operaciones.<br><br>El caso más frecuente podría ser la interrupción sorpresiva de una aplicación aislada.   | No tan buena. La estabilidad depende de una variedad de factores, como la configuración de programas y dispositivos físicos. La inestabilidad frecuentemente provoca fallos de sistema, como reinicios, pantallas azules y congelamiento. |
| <b>Compatibilidad</b>                            |  |   |
| 4) Compatibilidad con Windows 64 bits            | Si   | No, debido a los requerimientos de Microsoft PatchGuard (Protección para el parche del kernel)  |
| 5) Compatibilidad con Windows Vista              | Si   | No, la mayoría de los eventos no pueden ser interceptados en modo núcleo, por diseño.   |

Debido a la forma en que son diseñados, algunos desvíos en modo núcleo no permiten que un proceso sea interrumpido (congelado) en espera de la decisión de un usuario.

Es por eso que los cortafuegos en modo núcleo se ven forzados a asumir una salida predeterminada, que no siempre será la correcta.

En los casos de comunicación entre procesos, esa decisión probablemente sería "Permitir" en primer lugar, y después preguntar cuando la aplicación modificada intenta acceder a la red, si esto sucede.

Este procedimiento, se asemeja a la siguiente situación: invitar a un ladrón a entrar por la puerta principal, y luego asegurarse de que no deje abierta una puerta trasera.

Los desvíos en modo usuario, en cambio, ofrecen mayor flexibilidad para tomar una decisión correcta e informada, y para bloquear proactivamente la actividad maliciosa.  
Por ende, previene una infestación del ordenador en una etapa más temprana.

## La visión de Agnitum

En Agnitum, creemos que una simbiosis saludable entre ambos métodos crea una situación óptima para el usuario.

En Outpost Firewall Pro, utilizamos una técnica compleja, que combina ambos modos de desvío de procesos, usuario y núcleo, trabajando conjuntamente para crear una protección más fuerte y amplia.

Sin embargo, es importante comprender que es absolutamente erróneo pensar que el uso exclusivo del desvío de procesos en modo núcleo, puede abarcar el panorama completo de protección.

También se pueden desarrollar pruebas de fuga similares, para demostrar las falencias del modo núcleo.

Si la cuenta del usuario tiene derechos de administrador, los desvíos en modo núcleo pueden ser modificados, tanto por código malicioso, como por aplicaciones legítimas (por ejemplo, un programa válido de restauración de valores de la Tabla de descriptores de servicios del sistema, como STTDRestore, que tiene permiso para remover dichas interceptaciones, a menos que tenga denegado el acceso a la memoria de bajo nivel. AVZ es otro ejemplo.)

Por lo tanto, en nuestra opinión, es más apropiado que el cortafuegos combine ambos tipos de interceptación de procesos, y no que utilice un único método.

Esto lo volverá más proactivo, confiable y capaz de resistir las amenazas del mundo real.

Ninguna técnica aislada será tan poderosa como la utilización simultánea de ambas. Esa es la visión que promovemos en Agnitum.

## Síntesis

Para poder atravesar el desvío de procesos en modo usuario, así como en modo núcleo, es necesario utilizar técnicas de programación muy sofisticadas, pero ambos métodos poseen cierto nivel de vulnerabilidad.

El mejor consejo de seguridad que podemos ofrecer, es que no existe una solución cien por ciento efectiva.

Las técnicas más eficaces son aquellas que pueden manejar las amenazas que existen actualmente, combinando ambos métodos de control de comunicación entre procesos.

Ese ha sido siempre nuestro principio rector, y la causa de que sigamos creyendo que Outpost Firewall Pro es la mejor protección que un usuario puede tener.