

¿Por qué es efectivo el módulo anti-espía de Outpost Firewall Pro?

¿Por qué un anti-espía de Agnitum?

Detallaremos las razones por las que tiene sentido lanzar una protección anti-espía por medio del cortafuegos Outpost Firewall Pro.

La amenaza creciente de los programas espía

Los programas espía son un problema que se incrementa día a día y que ha afectado a muchos ordenadores personales. En un estudio realizado por National Cyber Security Alliance se calculó que 9 de cada 10 ordenadores conectados a Internet, están infectados con programas espía.

Aunque las definiciones detalladas sobre los programas espía aún permanecen algo confusas, se considera generalmente que la “etiqueta” espía alcanza a cualquier programa que:

- Se instala de forma encubierta, sin el conocimiento ni el consentimiento del usuario.
- Realiza modificaciones en programas existentes o en la configuración interna del sistema operativo.
- Puede mostrar publicidades que no fueron solicitadas.
- Puede permitir que se extraiga del ordenador información personal del usuario.

Los programas espía suelen evadir las herramientas de seguridad convencionales tales como antivirus y cortafuegos básicos, y quitarlos requiere de una tecnología especializada que no la proporcionan estas herramientas más generales. Los programas espía están diseñados para operar de forma encubierta en segundo plano y, para la mayoría de las personas, la presencia de los programas espía se siente sólo después de que el daño esté hecho.

La protección por separado ya no es suficiente

Hoy en día, muchos vendedores de seguridad ofrecen programas anti-espía autónomos que pueden detectar y limpiar programas espía de un ordenador ya infectado. Teniendo en cuenta que estas soluciones emplean lo que se denomina un enfoque reactivo (eso es, que tratan al problema sólo después de que se haya convertido en problema), estos productos apenas pueden ser considerados lo último en protección contra programas espía. Para que un anti-espía sea verdaderamente efectivo, es necesario que posea mecanismos proactivos (bloqueo preventivo) y reactivo (eliminación después de la detección).

Además, ya que la mayoría de los productos anti-espía autónomos se basan en definiciones, los usuarios están poco preparados para tratar con las amenazas de día cero y con los programas maliciosos menos conocidos para los cuales las firmas no han sido definidas — aún asumiendo que esos usuarios actualizan regularmente sus programas.

Outpost Firewall Pro combina la tecnología anti-espía y de cortafuegos

Outpost Firewall Pro de Agnitum proporciona una solución integrada de seguridad combinando la tecnología de protección del cortafuegos y contra los programas espía, así protege al ordenador contra las amenazas actuales y futuras de los programas espía. La combinación de ambos tipos de protección de amenazas le permite a Outpost lanzar lo último en soluciones para el problema de los programas espía.

¿Por qué es entonces, preferible una solución integrada que dos productos independientes?

- Coordinación de todos los mecanismos de defensa en un solo motor. Este enfoque mejora el funcionamiento interno de los módulos del programa, elimina el vacío de respuestas ante amenazas, resuelve asuntos de compatibilidad y contribuye a una operación futura más efectiva.
- Acceso a la administración, control y actualizaciones desde una única consola. Este enfoque mejora la efectividad y la utilidad del programa, ahorra tiempo y elimina la necesidad de realizar actualizaciones por separado.
- Menor carga para los recursos del ordenador. Se reduce el consumo de la memoria, y se optimizan el rendimiento del disco duro y procesador cuando se ejecutan menos tareas.

La protección proactiva de Outpost implica que aún antes que el programa espía intente contactar un ordenador, el cortafuegos lo detiene en el trayecto sin la necesidad de una identificación de amenaza específica. Cualquier programa malicioso presente en el sistema es detectado y eliminado por la tecnología reactiva en base a firmas.






Los escenarios de ataque de los programas espía y la forma en que Outpost protege a los usuarios

Outpost Firewall Pro proporciona una protección de múltiples capas contra los programas espía, troyanos, gusanos y cualquier otro programa destructivo. Aquí solo presentamos algunos ejemplos de lo que puede suceder y cómo el enfoque de Outpost protege al usuario:

Etapas de la invasión de programas espía




Etapa 1:

El programa espía se acerca al sistema objetivo, establece contacto, e intenta instalarse.

Cómo sucede		Cómo protege al usuario Outpost Firewall Pro
Se aprovechan de las configuraciones de seguridad inadecuadas en el explorador.		El complemento Contenido Activo de Outpost refuerza la seguridad en el explorador cerrando los canales de posible acceso por los que el programa espía podría ingresar al ordenador.
Ocultos en un archivo adjunto de correo.		El complemento Cuarentena de archivos adjuntos le permite al usuario poner en cuarentena los archivos adjuntos por clase de archivo, así evita que se abran accidentalmente los archivos que pueden estar infectados con programas espía.
Por medio de descargas desde los sitios Web que transmiten los programas espía.		El explorador de programas espía de Outpost le permite al usuario verificar cualquier objeto descargado y quitar cualquier programa espía de inmediato.
Empaquetados con programas benignos (programas demo, clientes P2P y otros).		la protección en tiempo real de Outpost mantiene una mirada constante sobre la actividad del ordenador y quita los programas espía inmediatamente después de detectarlos.
Aprovechando las vulnerabilidades del sistema.		El motor del cortafuegos de Outpost le permite al usuario crear reglas personalizadas especificando cómo deben manejarse las funciones de nivel de sistema y qué permisos internos pueden tener los componentes vulnerables. Ayuda a mitigar el problema antes que esté disponible algún parche por parte del fabricante.

Etapa 2:


Los programas espía infectan el ordenador y se afianzan profundamente en el sistema.

Cómo sucede	Cómo protege al usuario Outpost Firewall Pro
Los programas espía se activan en el ordenador 	La Protección contra programas espía en tiempo real de Outpost registra los programas espía en la memoria y detiene el proceso inmediatamente. Una vez que el proceso es desactivado, quita todos los rastros del código malicioso.
Partes de aplicaciones benignas ya instaladas son reemplazadas por un código malicioso (secuestro de la aplicación), que ejecuta al programa espía en lugar del programa "legal". 	Las funciones de Control de componentes y de Control de procesos ocultos y abiertos de Outpost permiten a los usuarios decidir si se le permite a una aplicación compartir datos con otra y comenzar procesos en su nombre, de esta forma, cierra un agujero utilizado con frecuencia por los programas espía para transmitir la información del usuario.
Las configuraciones de Windows y del Explorador son modificadas por programas espía insertados. 	Outpost, a través del control de componentes , rastrea las modificaciones efectuadas a los programas y muestra una ventana de alerta donde los usuarios pueden decidir si permiten que una modificación en particular tenga lugar.

Etapa 3:

Los programas espía ganan control e intentan completar su misión sin autorización.

Cómo sucede	Cómo protege al usuario Outpost Firewall Pro
Los programas espía envían información confidencial del usuario.  	El filtro de la aplicación del cortafuegos evita la transmisión de datos. El programa espía es identificado y eliminado por el módulo anti-espía, el cual también implementa un bloqueo de identificadores ID para evitar que cualquier información previamente definida salga del ordenador del usuario.
El programa espía muestra publicidades no solicitadas, abre múltiples ventanas emergentes, muestra contenido Web inapropiado o inesperado.  	El complemento Publicidades de Outpost bloquea publicidades basándose en el tamaño, en el emisor, o el tipo de animación, entre otras, y el bloqueador de publicidades emergentes (<i>Pop-up</i>) evita que se abran ventanas redundantes. El complemento Bloqueo de contenido habilita el bloqueo basándose tanto en palabras como también en la dirección de sitios o páginas de Internet.

 +  = 

Está claro entonces, que Outpost Firewall Pro con módulo anti-espía integrado protege a los usuarios contra los programas espía en todas las etapas del proceso de infección, salvaguardando efectivamente la información personal del usuario y manteniendo el rendimiento del ordenador sin problemas.