Introducción.

Patriot NG es una herramienta de tipo 'Host IDS' que permite monitorizar en tiempo real cambios en sistemas Windows.

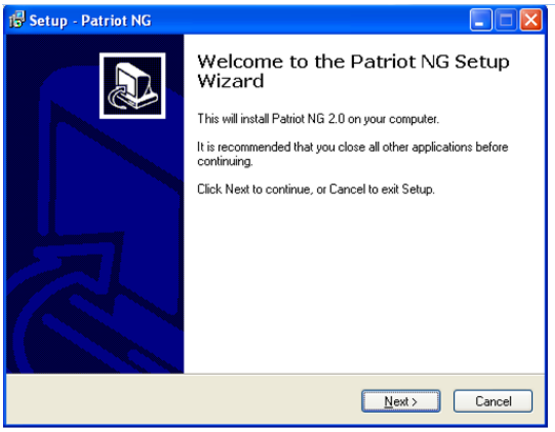
Según la wikipedia, se entiende por un IDS un programa usado para detectar accesos no autorizados a un computador o una red.

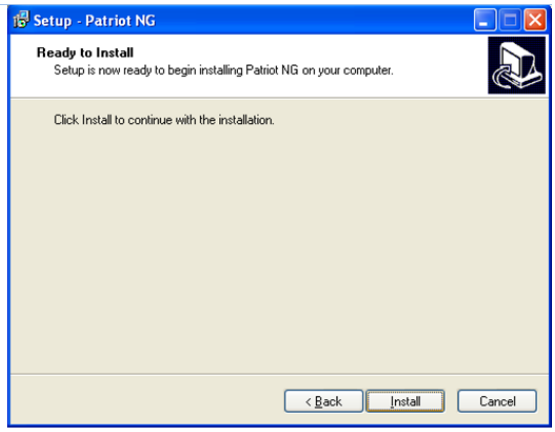
Condiciones previas.

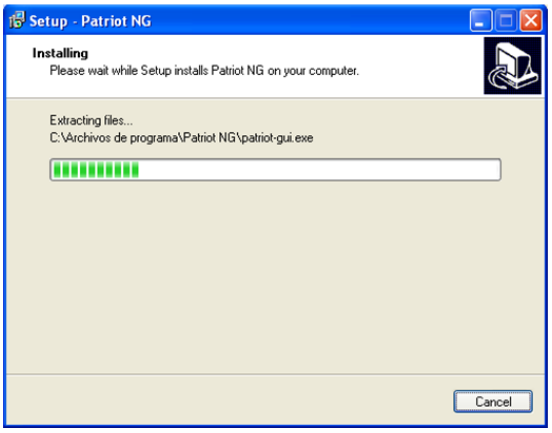
Es necesario tener instalado Winpcap (http://www.winpcap.org/install/default.htm) para ser completamente operativo.

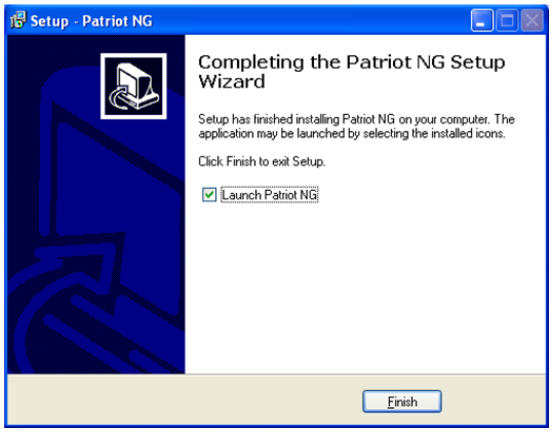
Instalación.

El proceso de instalación es extremadamente sencillo. Una vez ejecutado el instalador, se seguirán los pasos que indica el asistente.







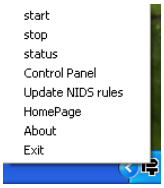


Con estos pasos ya está instalado el programa en el equipo. Se podrá comprobar viendo los iconos de los programas activos en la barra de tareas.

Este procedimiento es el mismo para cualquier versión de Windows (XP, Vista, 7).

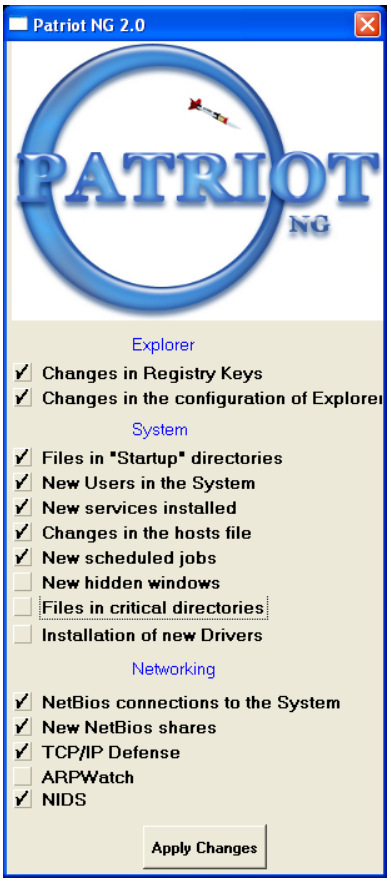
Opciones.

Una vez instalado, haciendo clic con el botón derecho sobre el icono de la barra de tareas nos aparecen las diferentes opciones que nos ofrece:



- Start: Inicia el programa en caso de que esté parado o bien avisa que ya está activo.
- Stop: Detiene el programa
- Status: Indica el estado en que se encuentra en ese momento.
- Panel de control: Se configura el comportamiento de la aplicación. Se explica con más profundidad en el siguiente punto.
- Update NIDS rules: Actualiza las últimas reglas de filtrado para Patriot.
- HomePage: Abre un navegador con la URL www.security-proyects.com
- About: Muestra pequeña ventana con la dirección email del desarrollador
- Exit: Sale del programa

Panel de control.



Las diferentes opciones disponibles son:

Explorer

- Change in Registry settings: Windows utiliza un sistema para almacenar la configuración llamado “registro”. En él se encuentran configuraciones que son alteradas por algunos programas maliciosos para infectar los ordenadores y asegurarse su ejecución al inicio del sistema. Esta protección monitoriza esas claves importantes y genera alertas cuando detecta modificaciones en ellas.
- Changes in the configuration of IExplorer: Una de las cosas que realiza el software del tipo Spyware es alterar la configuración de Internet Explorer para poder monitorizar el tipo de Webs que se visitan o para forzar que se visiten Webs no deseadas. Esta alerta avisa si se producen cambios en la configuración de Internet Explorer.

System

- Files in “Startup” directories: Windows dispone de unos directorios especiales conocidos como directorios “startup” donde se colocan ficheros para que sean ejecutados durante el inicio del sistema. Cualquier ejecutable que esté colocado en esos directorios será ejecutado durante el proceso de arranque. Muchos programas de tipo troyano emplean estos directorios para copiarse en ellos y de esa forma, asegurar su presencia en el sistema en cada arranque. Esta protección genera alertas cuando detecta que un nuevo fichero ha sido copiado en esos directorios.
- New users on system: Esta protección alerta si se crean nuevos usuarios en el sistema.
- New services installed: Un servicio es un tipo de programa especial que normalmente se ejecuta con los máximos privilegios. Suelen ser empleados de forma legítima para añadir funcionalidades a Windows. En algunas ocasiones, programas maliciosos se camuflan como este tipo de programas para infectar el sistema. Esta protección alerta si aparecen nuevos servicios en el inicio.
- Changes in the Hosts file: Windows dispone de un fichero llamado “hosts” en el que se pueden almacenar nombres de hosts y sus direcciones IP para que el sistema las tenga en cuenta de forma preferencial. Algunos troyanos o Spyware alteran este fichero para redireccionar maliciosamente conexiones a diversos hosts. Esta alerta avisa en el caso de que se produzcan modificaciones en este fichero.
- New scheduled jobs: Windows dispone de un sistema conocido como “Scheduler” o planificador por el cual se pueden programar tareas para que el sistema las ejecute. Existen programas malware que utilizan el planificador como forma de preservar su presencia en el sistema. Esta alerta informa si aparecen nuevos trabajos en el planificador.
- New hidden windows: Pueden ser generadas por algún proceso de instalación de una aplicación o como consecuencia de un ataque a nuestro equipo. Cuando se vaya a ejecutar cualquiera de ella, dará un aviso.
- Files in critical directories: Esta protección avisa si aparecen nuevos ficheros ejecutables en directorios del sistema.
- Instalation of new drivers: Algunos programas tipo rootkit (ocultan ficheros, procesos, conexiones) se instalan en el sistema como drivers, ésta alerta avisa si aparecen nuevos drivers instalados en el sistema.

Networking

- NetBios connections to the system: Esta protección alerta ante conexiones que se realicen contra nuestro sistema utilizando el protocolo NetBios (recursos compartidos). Generará alertas cuando alguien acceda a carpetas o archivos en nuestro equipo.
- New Netbios shares: Esta alerta avisa en el caso de que aparezcan nuevas carpetas compartidas mediante NetBios.
- TCP/IP defense: Informa de nuevos puertos abiertos, nuevas conexiones realizadas, ARP Spoofing...
- ARPWatch: Detecta nuevos host en la red.
- NIDS: Sistema para detectar tráfico anómalo que reciba el equipo. Se basará en un fichero de reglas configurable, para poder personalizar los patrones de tráfico según el entorno o la necesidad.