

Introducción

Patriot es una herramienta que monitoriza la configuración de Windows y alerta si se producen cambios significativos. Normalmente este tipo de cambios suelen deberse a la acción de software de tipo "malware" que engloba Spyware, Troyanos o dialers.

En el momento en que una variación es detectada, se muestra una alerta informando del cambio y ofreciendo la posibilidad de revertir ese cambio en la configuración.

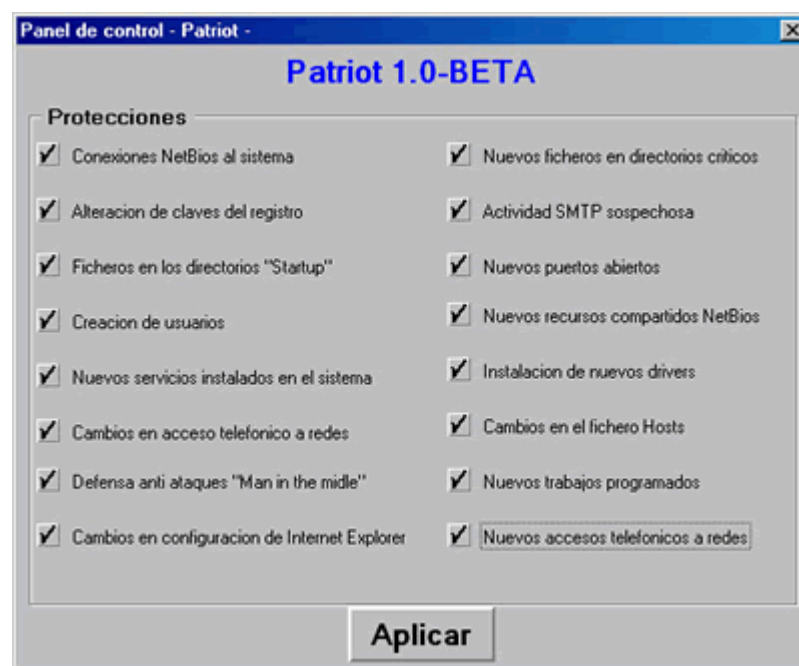


Fig.1: Panel de Control de Patriot.

1. Conexiones Netbios Al Sistema

Esta protección alerta ante conexiones que se realicen contra nuestro sistema utilizando el protocolo NetBios (recursos compartidos) Generara alertas cuando alguien acceda a carpetas o archivos en nuestro equipo.

2. Alteración De Claves Del Registro

Windows utiliza un sistema para almacenar la configuración llamado "registro", en el registro se encuentran configuraciones que son alteradas por algunos programas maliciosos para infectar los ordenadores y asegurarse su ejecución siempre que se ejecute Windows. Esta protección monitoriza esas claves importantes del sistema y genera alertas cuando detecta modificaciones en ellas.

3. Ficheros En Los Directorios "Startup"

Windows dispone de unos directorios especiales conocidos como directorios "startup" donde se colocan ficheros para que sean ejecutados durante el inicio de Windows. Cualquier ejecutable que este colocado en esos directorios será ejecutado durante el proceso de arranque de Windows. 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 de Windows. Esta protección genera alertas cuando detecta que un nuevo fichero ha sido copiado en esos directorios.

4. Creación De Usuarios

Esta protección alerta si se crean nuevos usuarios en el sistema

5. Nuevos Servicios Instalados En El Sistema

Un servicio es un tipo de programa especial que normalmente se ejecuta con los máximos privilegios. Este tipo de programas 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 Windows. Esta protección alerta si aparecen nuevos servicios en Windows.

6. Cambios En Acceso Telefónico A Redes

Un tipo de Malware bastante dañino es el conocido como "DIALER" Este tipo de software altera la configuración telefónica de Windows para que las llamadas se hagan a través de números con sobretarifación. Esta alerta avisa ante los posibles cambios en la configuración telefónica informando de los cambios y dando la posibilidad de revertirlos.

7. Defensa Ante Ataques "Man In The Middle"

Los ataques del tipo "Man in the Middle" son aquellos en los que mediante el envío de paquetes ethernet falsificados por parte de un atacante se altera la configuración de red para acceder y espiar el trafico. Esta protección avisa si se alteran parámetros de las tablas ARP y permite la opción de revertir el cambio.

8. Cambios En Configuración De Internet Explorer

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.

A close-up photograph of a white computer keyboard, showing several keys like 'P', 'F', 'D', 'X', and 'Z'. The keyboard is positioned on the left side of the page, partially overlapping a black vertical bar.

9. Nuevos Ficheros En Directorios Críticos

Esta protección avisa si aparecen nuevos ficheros ejecutables en directorios del sistema.

10. Actividad SMTP Sospechosa

Esta alerta avisa si aparece un número desproporcionado de conexiones a servidores SMTP

11. Nuevos Puertos Abiertos

Avisa si aparecen nuevos puertos TCP a la escucha.

12. Nuevos Recursos Compartidos Netbios

Esta alerta avisa en el caso de que aparezcan nuevas carpetas compartidas mediante NetBios.

13. Instalación De Nuevos Drivers

Algunos programas tipo rootkit (ocultan ficheros, procesos, conexiones) se instalan en el sistema como drivers, esta alerta avisa si aparecen nuevos drivers instalados en el sistema.

14. Cambios En El Fichero Hosts

Windows dispone de un fichero llamado "hosts" en el que se pueden almacenar nombres de hosts y sus direcciones Ips para que Windows 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.

15. Nuevos Trabajos Programados

Windows dispone de un sistema conocido como "Scheduler" o planificador por el cual se pueden programar tareas para que Windows las ejecute. Existen programas malware que utilizan el planificador de Windows como forma de preservar su presencia en el sistema. Esta alerta informa si aparecen nuevos trabajos en el planificador de Windows.

A close-up photograph of a white computer keyboard, showing several keys including 'P', 'F', 'D', 'X', and 'Z'. The keys are slightly raised and have a matte finish. The background is dark, making the white keys stand out.

16. Nuevos Accesos Telefónicos A Redes

Un tipo de Malware bastante dañino es el conocido como "DIALER" este tipo de software altera la configuración telefónica de Windows para que las llamadas se hagan a través de números con sobretarifación. Esta alerta avisa ante la creación de nuevos accesos telefónicos a redes.