Introduction.

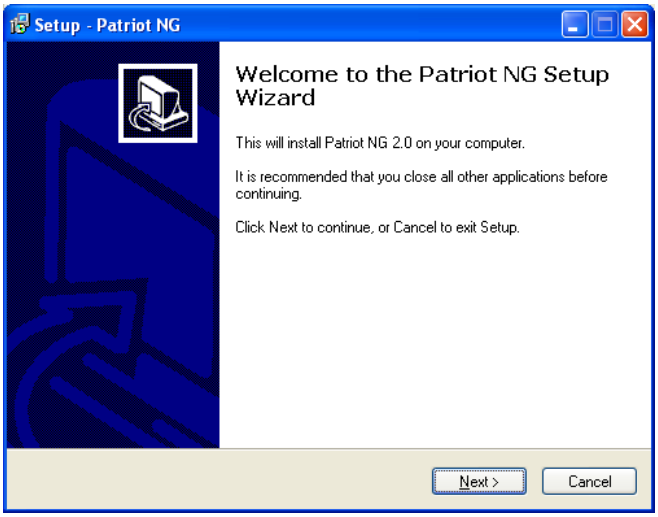
Patriot NG is a ‘Host IDS’ tool that allows real-time monitoring changes in Windows systems. According to Wikipedia, an IDS is defined as “a program used to detect unauthorized access to a computer or a network”.

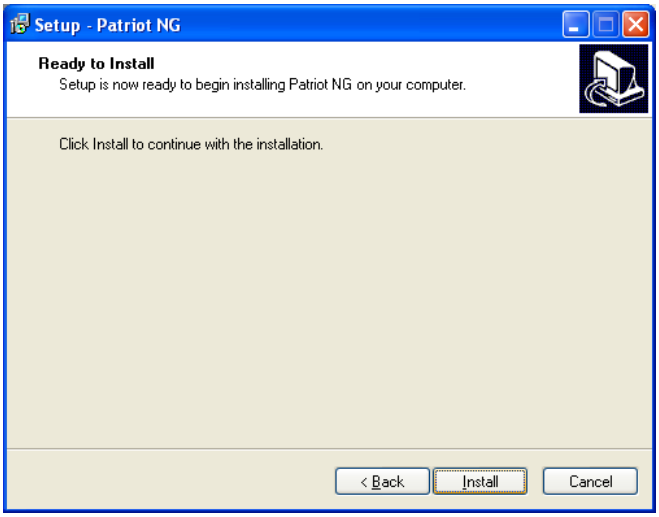
Prerequisites.

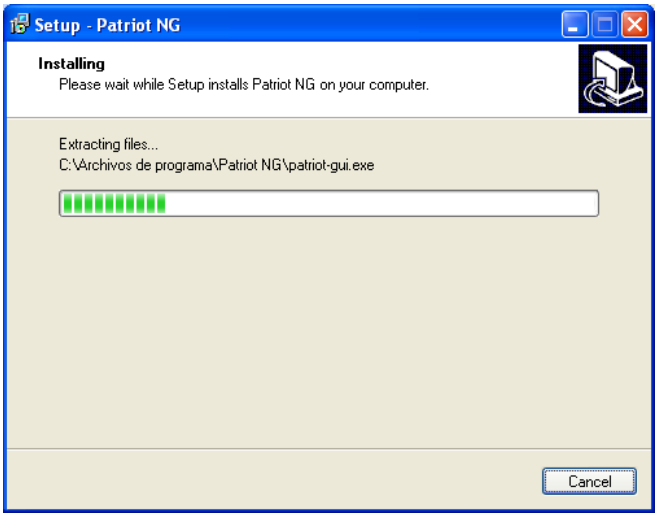
You need to have installed correctly Winpcap (http://www.winpcap.org/install/default.htm) to be fully functional Patriot 2.0.

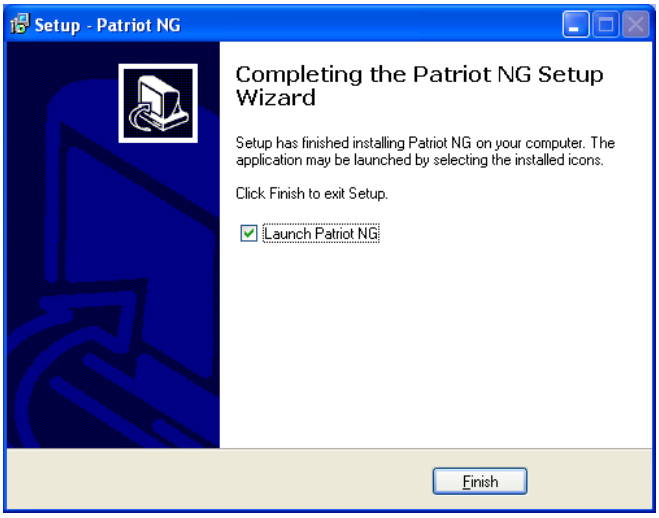
Installation.

The installation process is extremely simple. After you run the installer, follow the steps indicated by the wizard.







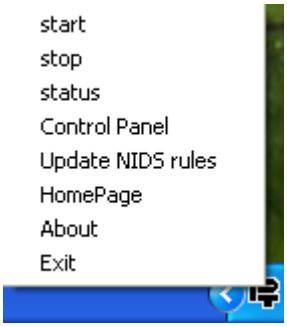


With these steps the program is already installed on the computer. It can be checked to see the icons of active programs on the taskbar.

This procedure is the same for any version of Windows (XP, Vista, 7).

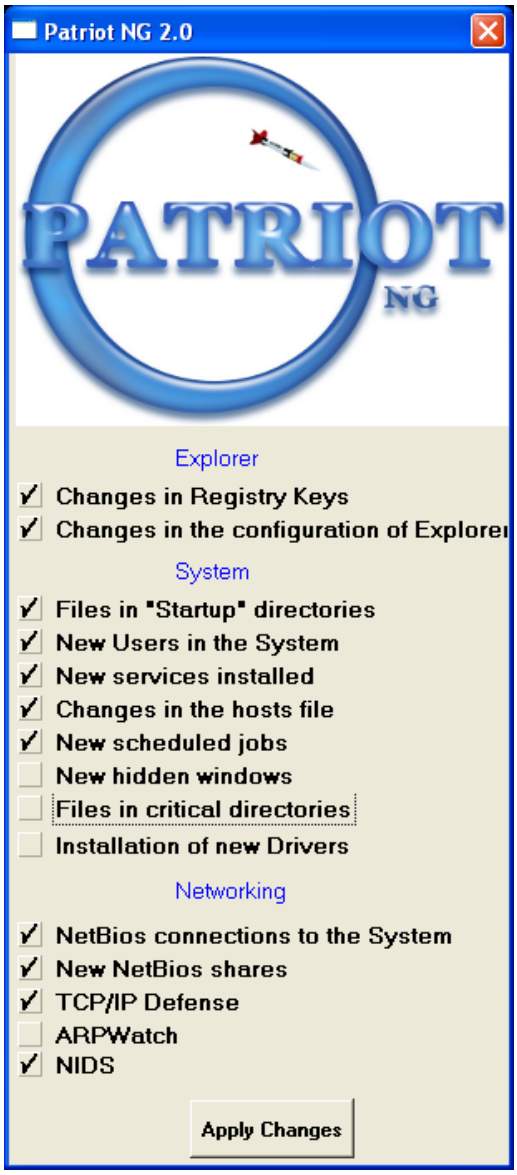
Options.

Once installed, clicking the right mouse button on the icon in the taskbar, a menu with the different available options will appear to us:



- Start: Begin the program if it is stopped or if it is already active will alert us.
- Stop: Halts the program.
- Status: Indicates the state at that moment.
- Control Panel: Configure the behavior of the program. It is explained in depth in the next issue.
- Update NIDS rules: Updates the latest rules for Patriot.
- HomePage: Opens in the browser the URL www.security-proyects.com
- About: Shows a small window with the email address of developer.
- Exit: Close the program.

Control Panel.



These are the different options available:

Explorer

- Changes in registry keys: Windows uses a system to store the 'registry' settings. It contains the settings that are changed by some malware to infect computers and ensure its execution on system startup. This protection monitors these important keys and generates alerts when it detects changes in their values.
- Changes in the configuration of Explorer: One of the things that makes the spyware is to alter the configuration of Internet Explorer to monitor the websites you visit or to force

you to browse unwanted websites. This alert warns if there are new changes in the Internet Explorer settings.

System

- Files in "Startup" directories: Windows has some special directories known as "startup" where files are located to be executed during system startup. Any executable file placed in these directories will be executed during the boot process. Many Trojan Horses use these directories to be copied to them and thus ensure their presence in the system at every boot. This protection generates alerts when it detects a new file has been copied into these directories.
- New Users in the system: This protection alerts if new users are created in the system.
- New services installed: A service is a special software that normally runs with the highest privileges. Usually employed in a legitimate way to add functionality to Windows. Sometimes malware camouflage themselves as such programs to infect your system. This protection alerts if new services are added to Startup.
- Changes in the hosts file: Windows has a file called "hosts" that stores hosts names and IP addresses for the system to take them into account preferentially. Some Trojans or Spyware alternate maliciously this file to redirect connections to different hosts. This alert warns if there are changes to this file.
- New scheduled jobs: Windows has a system known as the scheduler or planner through which can be programmed to run. There are malware programs that use the planner as a way to preserve their presence in the system. This alert advises if new jobs are added to the scheduler.
- New hidden windows: This windows may be generated when installing a new application or as a result of an attack on our computer. Whenever they occur, Patriot will warn us.
- Files in critical directories: This protection alerts us if new executable files as created in system directories.
- Installation of new Drivers: Some programs like rootkits (hidden files, processes, connections) are installed in the system as drivers, this warning alerts whenever any new driver is installed on your system.

Networking

- Netbios connections to the System: This protection alert to connections that are made against our system using the NetBios protocol (shares). It will generate alerts when someone access to the folder or files on our computer.
- New NetBios shares: This protection warning of a new share on the computer.
- TCP/IP Defense: Reports new open ports, new connections, ARP Spoofing.
- ARPWatch: Detects new hosts in your network
- NIDS: (Detect anomalous network traffic based on editable rules)