Invasion or Privacy

While the Internet is a wonderful new world with all the information it makes available, all the new communication channels and its ability to disregrad geographical borders and time zones, it has brought along with it a new breed of crime - invasion of privacy.

Basically, invasion of privacy falls into two broad categories, actual invasion of your privacy and, DoS (Denial Of Service), which doesnt compormise your private information but does deny you the right to be on the internet through various means. Many programs and tools have been written to prevent such attempts, but most have either proved too expensive and served mostly to cage in the person they are protecting (like firewalls) while others offer a temporary and incomplete solution.

Invasion of privacy

Where invasion of privacy is concerned, there are several programs available on the internet that allow intruders to achieve thier purpose. Back orifice, NetBus, GirlFriend etc are all such examples. They come in two parts, a client, which the Hacker/intruder uses, and a server which will reside on the victims Computer. Most come pre-configured to attack the victims PC on specific port numbers and install themselves in the Windows Regisrty using predefined paths. This is where most Security programs can detect/remove such malicious servers. The problem arises when the Intruder has some degree of skill and can change the port number he chooses to attack and/or the path in the windows Registry. His attempts will in most cases be rewarded and undected by most if not all Detection/Removal programs.

In effect, there is no way to totally prevent a determined and professional hacker from accessing your system by simply blocking known access ports.

FireEyes doesnt protect your PC from intrusion. It gives you the chance to see who IS accessing your PC and make up your own mind wether its a legitimate connection or a suspect connection. It also alerts you when ports or IP numbers you define connect to you.
This is probably the most realistic way of protecting your PC, it ensures you always KNOW when your PC is being accessed.

Connections

When connecting to the Internet, there a few terms you need to get used to.
- IP number
- ISP
- TCP/IP & UDP
- Port number
- Domain

IP Number

IP Number is a random number you get assigned when you dial in. Its random in that you cannot know in advance what the number will be exactly but it will fall in a range that your ISP owns. Please see below. Once connected, you will be identified to the Intenet as THAT number.

ISP

An ISP (Internet Service Provider) is what you dial into to connect to the internet. ISP's own a range of IP numbers called blocks. For example, an ISP might own the IP block or range
from 134.1.0.0 to 134.1.255.255]. If you are subscribed with that ISP, when you dial in, you will be assigned an IP from that range, for example 134.1.140.12. The next tiem yuo dial in you might get an IP like 134.1.127.123.

TCP/IP & UDP

So as not to get too technical, just consider them applications or programs that connect Computers on the internet together. The difference between both is that TCP/IP is more reliable. It attempts to connect one IP (your Computer for exmaple) to another IP (Computer). It knows if the message was sent or not and might re-try to conenct or inform you of the connection failure. UDP does the same as TCP only it doesnt check if message got through or not and hence is not so reliable. You will never need to worry about which to choose. Programs you use will already use one or the other. For Example netscape uses TCP/IP. UDP is mostly used by PING and ICQ when a user isnt online or visible and is sending messages to another user.

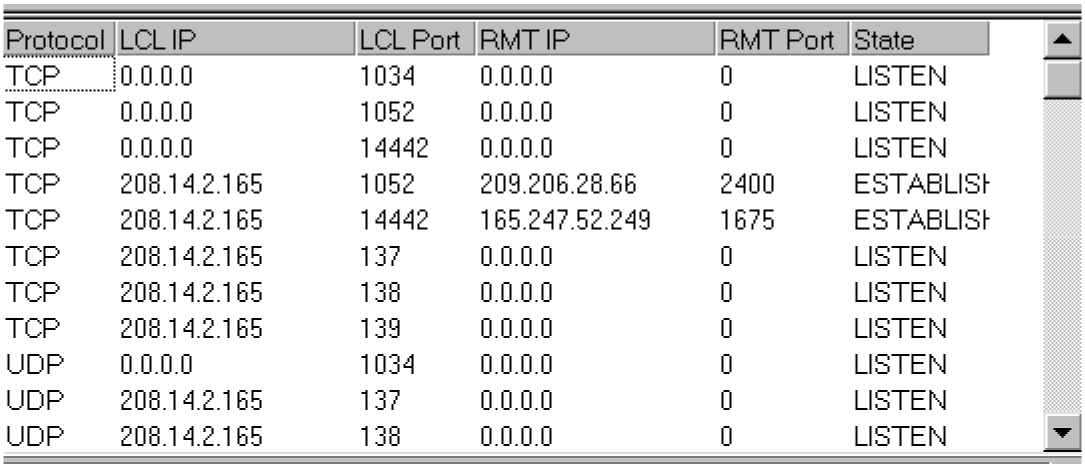
Port Number

These arent real ports, they are really windows files. When one IP (Computer) using TCP or UDP connects to another IP (another Computer) it does so through a port number on its own Computer and connects to a port number on the Other Computer.
For example, if you had an IP 165.176.1.2 and you where surfing to Yahoo to browse for example, your browser would automatically issue a TCP/IP request to connect to Yahoo. It would do so throught a port on your Computer (A random available port) say 1423 to one of Yahoo's static IP's say 204.71.200.74. It will connect to Yahoo on ITS port 80.

So 165.176.1.2, from its port 1423 would connect to to 204.71.200.74 on its port 80.
Your port is refered to as Local Port and Yahoos port is refered to as Remote port.
Some services use standard ports. For example most Browsers will connect to a remote port of 80 or 8080. FTP will connect on port 21, etc.

Domain

Domains or domain names are just friendly ways of addressing IP numbers.
www.webcruizer.com is easier to remember than 206.152.93.100. Internet servers have programs calls DNS's that will accept domain names and convert them to IP numbers internally.



Protocol	LCL IP	LCL Port	RMT IP	RMT Port	State
TCP	0.0.0.0	1034	0.0.0.0	0	LISTEN
TCP	0.0.0.0	1052	0.0.0.0	0	LISTEN
TCP	0.0.0.0	14442	0.0.0.0	0	LISTEN
TCP	208.14.2.165	1052	209.206.28.66	2400	ESTABLISH
TCP	208.14.2.165	14442	165.247.52.249	1675	ESTABLISH
TCP	208.14.2.165	137	0.0.0.0	0	LISTEN
TCP	208.14.2.165	138	0.0.0.0	0	LISTEN
TCP	208.14.2.165	139	0.0.0.0	0	LISTEN
UDP	0.0.0.0	1034	0.0.0.0	0	LISTEN
UDP	208.14.2.165	137	0.0.0.0	0	LISTEN
UDP	208.14.2.165	138	0.0.0.0	0	LISTEN

For further clarification, please look at the typical output from FireEyes above.
At the Left the label "Protocol" indicates wether the connection is TCP or UDP.
Next, the Label "LCL IP" indictates local IP which means you. This would either be your actual IP, or an internal IP. Internal IP's are either 127.0.0.1 or 0.0.0.0. In all cases ANYTHING under this label means YOU. Following that, the label LCL Port, indicates Local port - YOUR port. The two Lables after that indicate who is connected to you, RMT IP is the Remote IP connected to you, this could be anything, a Server like altavista.com, an ICQ online user an FTP Site or a hacker even. Then comes RMT Port, Remote port. This is the port thats on the PC connected to you.

So for example, looking at the 4th line from the top, a Computer that has IP 209.206.28.66 is connected from ITS port number 2400 to your computer on your port number 1052.

Next comes the label "State". This indicates the state of the connection. There are two states you should worry about. "Established" and "Listen". Established means the connection is in effect. If you know whose IP is connected then no problem.
"Listen" means some program on your system is running and has the indicated Local port open and waiting for a connection. This is something you have to investigate immeadiatley.
Only a few programs would do that. ICQ Listens that way, your own UDP ports listen that way awaiting pinging, nuke nabbers (like SynCity) do that and also BAck doors (Programs that are designed to give access to your computer do that. Notice that the "LISTEN" lines have no remote port or remote IP, simply because there are none, no one is connected yet. Programs open these ports and wait for a connection on them.
Though, as mentioned before, you need to investigate this immeadiatly, it doesn always mean that there is a malicious program on your computer, it may be one of the perfectly legitimate programs mentioned above.

What you should do is, while keeping FireEyes running, shutdown ICQ, this would remove a few "LISTEN" ports, shutdown any nuke nabbers, shutdown any email programs. Then click refresh on FireEyes. See which ports remain in the "LISTEN" State. If none remain, then at least you know you had nothing to worry about.
If some remain, then put those ports on your "watch list". FireEyes will Alert you as soon as these ports are accessed by any Computer. You can then check the IP number of the connection and find out Who/what it is and why its connected to you.

Briefly

Back doors, sometimes loosely refered to as Trojans, give someone access to your Computer. At times this access is as complete and total as though they were sitting at your PC. They can read/change your personal files, extract personal information from your registry, this includes name address phone number, what ever you entered. They can read your keystrokes as you type. They can even TYPE instead of you.

Back doors come preconfigured to "LISTEN" on certain ports. As soon as you start your PC, they will run and open those ports and wait in a "LISTEN" state for a connection. If who ever introduced this back door into your system did not customize it, it will remain using the predefined Port number. Here is where you are in more danger than you would be if the hacker was more skilled and had customized the port number. A pre-defined port number is known to all. For example, Back Orifice uses port 31377 by default. Now, ANY hacker on the Internet can gain accidental access to your system. Most Back doors have a tool called an IP Scanner. This means you specify a range of IP numbers to scan and test if the default port is open. If your IP number is in that range and you have a back door, chances are the hacker will gain access to your PC. Putting suspect LISTEN port number on the Watch list will alert you when and if that port is accessed.

There are many kinds of back Doors, Back Orifice, NetBus, Girl Friend, Paradise and more. Its no chore for a skilled tehnical person to write one in a week or a little more.
To avoid getting back doors, try not to accept GIF picture files from anyone, dont download or accept executable files or programs (.exe) or DLL (.dll) or documents (.doc) from anyone or any suspect site. Download only from reputable well established sites. Avoid Joke programs. In doing so you will also avoid Virii which are transmitted in the same manner.

Running

To run FireEyes, simply click the desktop icon or locate it in the Programs list and run it.
Once, running, you will find its icon on the task bar (bottom right of your screen) next to ICQ and other task bar icons.
To close FireEyes,or choose Exit on the program itself, or "right" mouse click Its task bar icon and choose exit.

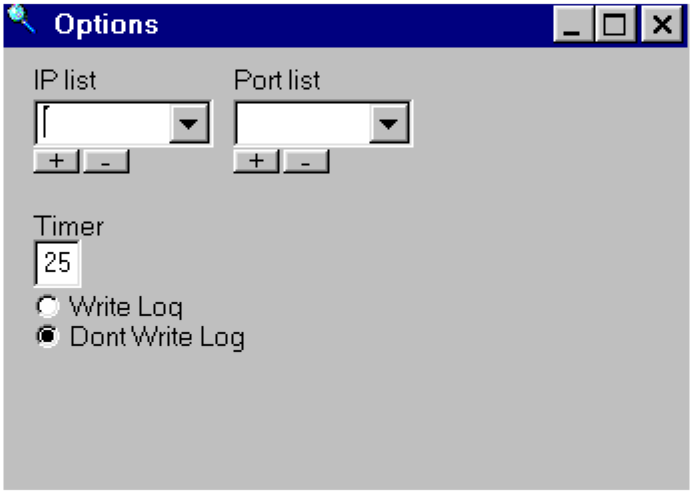
Important: FireEyes checks for new connection every "Refresh" Period. The Default Refresh Period is 25 seconds. You can set that to any value you choose from the Options Menu. Setting hte Refresh period too small would slow down your Computer, setting it to High would make it miss connections. The best value is between 30 seconds and 1 minute.

While running, FireEyes will allert you of any new connections made, These will either be Casual connections or "Watch List" Connections. Casual connections are displayed in Blue letters, Watch list connection are displayed in red Letters.

Because your prime concern is Invasion or prviacy, keep an Eye on all lines that have a state of "LISTEN" on them. They should be only ICQ ports, Nuke Nabber ports, email program ports and not much else.
To find out, while FireEyes is running, Shutdown ICQ, and any email program (eudora for example), and nuke nabbers and hit refresh (f5) to force an instant refresh. See if there are Still any ports in LISTEN state. Appart from LOCAL ports 138 and 139 (The windows UDP ping ports), there shouldnt be any. If there are then you will need to investigate what they are, you are also advised to put those LISTEN ports on the Port Watch List. This way FireyEyes will alert you once these ports are Connected to anyone on the outside.

Options

There arent many functions in FireEyes, basically, it is mainly output and putting IP's and Ports on the Watch list.



Timer 25

○ Write Log
● Dont Write Log

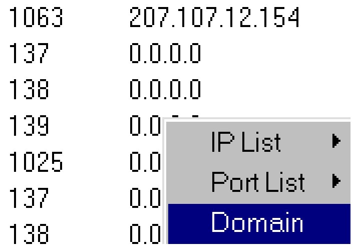
IP List
Enter IP numbers to watch here and click the "+" button do add them. You may also remove IP numbers from the Watch list by scrolling down in the IP List boxt and clicking the "-" button.
IP numbers are stored in an internal file and will be loaded when you run the program again.
Please remember that you dont need to enter the whole IP number. Infact its in advisable to do so. When ever a person logs on to the internet, they are assigned an IP number that is available from the ISP's IP block (see the section Connections). So if you are watching a specific IP number from an hour ago, the hacker might have disconnected and re-dialed and gotten another one. What you should do is put "some" of the IP numbers digits on watch. For Example:
IF a suspect IP number (163.200.173.14) connected to you.
If you put that whole number on watch, the Hacker might disconnect and redial this time getting the IP 163.200.118.56. FireEyes will be watching another IP alltogether and would not spot him.
If on the other hand you put 163.200 only in the Watch list, FireEyes would spot his new connection attempt and warn you.

Port List
Works the same way as IP List above except it watches YOUR (local) ports. Ports to generally lookout for are 12345 12346 (NetBus) 31337 31336 (BO). Ofcourse there are more, but these are default ports and you should always keep an eye on them.

Popup Menu
The popup menu is activated by placing the cursor on a specofic line and clicking the RIGHT mouse button. A popup Menu will appear. FRom hte menu y can add/delete the IP number or Port Number on this line directly instead of going to the options menu to do so.
Also, If you click on Domain, the IP number on that line wil be resolved into its domain name.

Timer
FireEyes works by taking a "look" at your connections. It does so every "Timer" time. So if Timer was set to 30, FireEyes would check your connections every 30 seconds.
A good value is 30 seconds, even 1 minute is acceptable. If you set this value too low, your system will

slow down, if you set it too high, you will miss connections attmepts.
Connections dont last too short a time, even after the connection is made and ended, TCP/IP still maintains a n entry for it in one of other states, like "CLOSED", so you will still see it.



```
1063      207.107.12.154
137       0.0.0.0
138       0.0.0.0
139       0.0
1025      0.0
137       0.0
138       0.0
```

Known Bugs

Two bugs remain un resolved which may or may not appear on ur system

1) You may expereince a slow down of your system after running FireEyes for a while
Simply close it and open it again

2) You may get the message "system out of resources". This is due to windows not Freeing the memory used by the time correctly. Again, close FireEyes system and open it again. Also set the snap shot time to a larger value like 1 minute

Getting Support

Please report any problems to software@webcruizer.com