Title:
How To Stop Spyware

Word Count:
755

Summary:
This is an additional method that should be used in conjunction with an anti-spyware product.

How can this method prevent spyware from "calling home" with your personal information? It works by letting Windows filter the IP addresses that you place in the hosts file.

What is the host file and how does it work?

The host file resides in the Windows folder on your hard drive and it loads into system memory each time the computer is turned on. For each IP address that is...

Keywords:
Spyware,information security

Article Body:
This is an additional method that should be used in conjunction with an anti-spyware product.

How can this method prevent spyware from "calling home" with your personal information? It works by letting Windows filter the IP addresses that you place in the hosts file.

What is the host file and how does it work?

The host file resides in the Windows folder on your hard drive and it loads into system memory each time the computer is turned on. For each IP address that is placed in the hosts file, it is cross-referenced with a saved domain name.

Siince the Internet only understands numeric IP addesses, this cross-referencing with domain names is required. These translations between IP addresses and domain names reside on various Domain Name Servers (DNS) that are distributed around the Internet.

IP addresses are in the form of a block of numbers arranged in quartets as in the following example: 125.0.48.220.

They way it works is, as you enter a domain name (URL) in your browser, the first thing that happens is that your computer will check for any IP addresses that are in your hosts file. If it finds the relevant domain name, it will not bother searching the external DNS servers on the Internet.

Before there was the current high-speed connections that we use everyday to connect to the Internet with, it was quicker to find an IP address that was stored on the local computer.

Once you activate a link that is associated with Spyware, by clicking on it, or sometimes just moving the mouse over it, the Spyware in most cases attempts to "call home" back to its server somewhere on the Internet. It can then create an ad server, scrape your personal data and send it back to its server.

Since we now have faster Internet connections, the need for hosts files have just about been eliminated.

Whenever you run into a malicious domain, just add it to your hosts file, and instead of cross-referencing it to a valid IP address, translate it to a fake IP address that connects to a void inside your computer. Then the Spyware thinks it is calling home to its servers, however the call goes nowhere.

The hosts file has entries in it with the following format:

```
#hosts file from windows directory
127.0.0.1 localhost
123.45.67.89 testsite1.com
51.126.0.189 testsite2.com
```

The # sign indicates comment lines that the computer will ignore.

In using the hosts file as a Spyware or adware blocker, you will always see the localhost setting in the first line of the file.

Notice that these IP addresses are all the same: 127.0.0.1 -this points only to your own local computer.

You will also see the all of the other IP entries will have the same address as the localhost, as in the following example:

```
# host file from windows directory

127.0.0.1 localhost
127.0.0.1 testsite1.com
127.0.0.1 testsite2.com
```

When an infected webpage tries to connect your computer to testsite1.com, the browser looks up the IP address for testsite1.com, and in this situation will find it in the hosts file. Since the IP address translates to 127.0.0.1, the call cannot go out back to its server out on the Internet.

This works simply because the domain is stored on the local computer in the hosts file and Windows will not try to resolve it on the external DNS servers.

Using this methodology will also reduce the time is takes to access normal web pages since it does not have to wait for all of the ads and images to download.

This should not be used as the only solution for Spyware. It should only be used with another proven Spyware product.

The steps with this procedure are not straight-forward as one might think. You have to:

a) detect each bit of Spyware
b) look up the domain name
c) modify the hosts file for each event

It is a constant struggle because not only are companies who produce Spyware and spam are always adding new domain names.

You should not be discouraged however, since you can download very detailed hosts files from the Internet that do not have any costs associated with them. You can visit specific sites that offer this service and download their files. Just remember to constantly check and download the latest updates to these files.

You can also let an anti-spyware program do it for you, such as SpyBot. It will automatically include these problem sites in your hosts file.

For more information on hosts files, simply search on the term in Google