

## Understanding Spyware, Browser Hijackers, and Dialers

### Introduction

For the past couple of years there has been a new threat introduced to your computer that anti virus software does not as of yet remove. This software is developed to track your movements on the Internet, create statistics of what you do on your computer, or even worse, actually hijack your web connections to direct you to pages that you did not ask for. These types of programs are called Spyware, Browser Hijackers, and Dialers.

Before we define Spyware, Hijackers and Dialers it is important to understand another type of program called **Adware**. Adware are programs that are usually free, otherwise known as Freeware, that have advertisements built into the software. That means when you run the software, it will pull down advertisements from the Internet and display them somewhere in the software. Most of these types of software allow you to register the software, by paying some fee, in order to remove the ads.

**Spyware**, on the other hand, are pieces of software that are advertised as Freeware or Adware but that install in your computer, generally without your knowledge, other programs that run in the background collecting data about what web sites you go to, your personal information, the games you play, the software you use, etc, all without your permission. The software will then send this information back to the creator's servers where it is collected.

There are many different types of Spyware and a few are described below.

### Adware Networks

Ad networks are companies that pay software developers and web sites money for allowing their ads to be shown when people use their software or visit their sites. These ads are generally in the form of popups and present you with some sort of advertisement. The problem with these networks is that they place cookies on your computer each time you open an ad served by the particular network. This allows the advertising network to track your movements across the Internet by reading the information contained in the cookies every time you connect to a site that they are on. Networks that employ this method are ones like Double Click, Value Click, Gain, and Radiate.

### Backdoor Santas

These are programs that you download off the Internet and contain valid uses. They do though, collect statistics of your computer use, the sites you go to, the type of hardware, etc and transmit this information back to their servers. They generally do not work with adware networks. Programs of this type are Comet Cursor, Alexa, Hotbar, and Cuteftp.

#### Stalking Horses

These types of spyware are generally bundled into many popular programs and often, but not always, are presented in the installation as desirable additions to the main software, the trojan horse, that you are installing. Example programs of this type are EZula's TopText, Cydoor, Onflow, and Webhancer.

#### Trojan Horse.

These types of software are usually very popular downloads and are free downloads. They almost always contain at least one Stalking Horse and software for ad-serving networks. Many times you are given the option to install these stalking horses or ad-serving program, but they are sometimes hidden in the fine print of the Trojan Horses License Agreement. In some situations, if you choose not to install the Spyware, you will not be able to use main program or Trojan Horse. Examples of programs that are Trojan Horses are KaZaA Media Desktop, Grokster, and Morpheus .

There are other types of malicious software that can be installed on your computer. They are described as follows.

### **Browser Hijackers**

Software that tends to Hijack your browsers web connections to do their own purposes. They will change your homepage to another homepage no matter how many times you change it or you can do a search in Google, but instead of getting the results back from Google, your search request is actually hijacked and sent to another search engine.

### **Dialers**

Software that gets installed on your computer that has the ability to make phone calls from your computer, if you have a modem, without your knowledge. These programs will connect to other computers, through your phone line, which are usually porn sites. These numbers are pay per call though, so you get charged for the amount of time your computer is connected to it

### **Malware**

Software that gets installed on your computer without your knowledge that changes system settings, not limited to your browser settings, that cause harmful effects to occur on your computer.

It is also important to note, that practically all Spyware and Hijackers tend to target Internet Explorer and not other browsers such as Netscape or Mozilla Firefox. If you are not against switching your browser, then you can switch to an alternate Web Browser and immediately greatly reduce your risk of infecting your computer with one of these programs. If you are willing to switch browsers, I would recommend [Mozilla Firefox](#).

### **Why do people make these programs?**

The simple answer? To make money.

A big trend during the Internet boom was to provide free software to downloaders. Why would they offer it for free? It is because these programs would gather statistics about the users activities on the Internet or on their computer, what hardware they have, what software they use, etc. Then they would sell this information to third-party organizations without your knowledge. This type of information gathering via a piece of software without knowledge is called Spyware.

Hijackers are another newer breed of software that literally takes over control of certain operations of your web browser. By doing this they can redirect browsers to sites of their choice where they may gain a commission for the user going there or to increase traffic to their site generating higher ad revenue. Even worse, these Hijackers can redirect search results from their own search engines to you, when you do a search on a popular search engine like Google.

Dialers make their money by having your computer connect to numbers where you get charged exorbitant fees while you are connected.

### **How do you get Spyware, Hijackers, and Dialers?**

The most common method of being infected is to not have the proper security settings in your browser. Internet Explorer is generally targeted the most by Spyware/Hijackers and unless you have the browser's security settings configured properly, you will have a good chance of getting infected with something. We will discuss later methods of securing your browser.

Spyware can also be installed via programs downloaded off of the Internet, through cookies when you connect to a site, or from site popups that ask you to install something. The programs downloaded off the Internet are generally free downloads, as they know that the revenue from the information gathering will offset the cost of giving it for free. A lot of times, you can read the privacy policy of a piece of software before you download it. It will sometimes note that software will be installed on your computer than gathers information about your activities and sends it back to them. It is your choice at this point if the usefulness of the software outweighs your loss of privacy.

Certain Internet advertising companies such as Valueclick or DoubleClick will install cookies on your computer every time you load one of their advertising banners. These cookies, which are small files that store information from a web site between visits, allow them to see what sites you go to and what you do on these sites. Though cookies can be used to gather information about you, they are also used for valid reasons when visiting many sites. Therefore disabling cookies, could cause loss of functionality to sites you may frequent.

You can also get spyware from a popup that you see at a web site asking if you would like to install their greatest and latest piece of software. Use extreme caution when accepting these types of offers.

Hijackers and Dialers, on the other hands, are almost always installed by going to a site where you will see a popup displayed saying that you must have this new piece of software that only they can provide to you. The most common popup scams are:

When they say you have a security hole and to click here to fix it.  
Software that makes you able to connect to sites faster.  
You have open ports on your computer! Click on the ad to download a utility to fix it.  
Ads that say they can make your computer run faster.

It is not unheard of for these programs to even install themselves just by reading an email, though proper security updates and patches can minimize if not eliminate this risk.

Though, these programs can install themselves on your computer via these methods, that does not mean you should panic and throw your computer out. It does mean, though, that you should pay attention to what you click on and read the fine print. Even more important, you should add a Spyware checker and Removal software, like Spybot, into your routine for protecting your computer like you already do with virus scanning.

### **How do I know if I have Spyware or a Hijacker on my Computer?**

There are only two ways of knowing if this type of software is installed on your computer.

The first way is if you notice your web browser behaving strange. Some common symptoms are :

Your home page changes on its own.  
You can not change settings in your browser.  
Your search results seem strange.  
You have toolbars on your web browser that you did not install.  
You are getting a lot more popups.  
Your browser suddenly starts crashing.

If you have any of these symptoms then you most likely have a some sort of Spyware or Hijacker installed on your computer.

The second way of detecting spyware is to use a Spyware removal program routinely and let it search through your computer and optionally remove any spyware if it finds them. It is sad, but with how bad these programs have become, running Spyware Checkers routinely as you do a anti virus program is really a requirement these days.

### **How do I remove Spyware and Hijackers?**

A word of caution before you use any of these programs. Spyware is sometimes tightly integrated into other legitimate programs that you use and disabling them could cause those programs to no longer function properly. For example, Kazaa, which is a popular file sharing service, installs spyware into your computer when you install it. By removing this spyware, Kazaa will no longer

work. In my opinion, removing the spyware and preserving your privacy is more important than using the programs that install them, but it is ultimately your choice to decide which is more important.

**Spybot - Search and Destroy** is an excellent utility. It will search your computer for any known Spyware and Hijackers and remove them from your system. It does this by scanning your registry, files, cookies, and other storage places against a large database of known offenders. When it finds a Spyware/Hijacker it will present it in a list of others that if found and allow you to choose which you want to delete. You can then have Spybot remove these entries and delete the files.

You can download this Spybot here: <http://www.safer-networking.org/index.php?page=spybotsd>

**Ad-Aware** is another excellent piece of software for removal of Spyware and Hijackers. It has the same features as Spybot, but was one of the first programs to be created for removal of these types of programs and is recommended that you scan with this software as well as Spybot.

You can download Ad-Aware here: <http://www.lavasoftusa.com/support/download/>

### **How do I prevent myself from getting infected again in the future**

The first step before you protect yourself from future infections, is to first clean your system using the above utilities. If you have not done this as of yet, please do so, and then continue reading this section.

Once you feel you are clean, you should Immunize your system. What that means is that you tell Windows certain programs that it is not allowed to run. This protects you because if you go to a site that attempts to install malicious software, it will not be able to because the operating system has been told to not allow that particular program to be able to run.

Spybot -S & D offers an immunize feature that will protect your computer as was discussed above. Unfortunately new variants of Spyware/Hijackers tend to get let loose in the wild often so be sure to allow Spybot - S&D to update it's database of known malicious programs very frequently.

### **Conclusion**

As you can see Spyware and Browser Hijackers are becoming a serious problem for a computer users. With proper use of the tools at your disposal, though, you can safely remove these programs from your computer.