TDDC03 Project, spring 2007

# Security and Usability of Anti-spyware software

**Syed Zahid Ali, Kristoffer Lundholm**

**Supervisor: Almut Herzog**

# Security and Usability of Anti-Spyware Software

Syed Zahid Ali Kristoffer Lundholm
*Linköpings universitetet, Sweden*
*Email: {syeal477, krilu224}@student.liu.se*

## Abstract

*These days the Internet is getting more and more hostile to unsuspecting users. There are a lot of programs and web pages on the Internet that will try to install Adware/spyware on end users' computers. These threats come in all forms from simple tracking cookies to resource hungry spying programs designed to steal users' online identity. The more dangerous programs cannot be uninstalled by using the Windows add/remove program function and therefore we need special anti-spyware programs to detect and remove this type of threat.*

*In this report we have evaluated five different anti-spyware products by installing them on a personal computer and then test them against our proposed security criteria. We also discuss some usability features of the programs tested. After downloading and testing the five different anti-spyware programs we have seen that none of them is perfect and provide full protection against the spyware. Finally there are recommendations for end users how to avoid getting infected with spyware in the first place and if they get infected what to do.*

## 1. Introduction

The name spyware covers several different types of software that are designed to gather personal information about computer users. How this information is used depends on what the installed spyware was designed to do. Some spyware just creates a profile of the user's surfing habits and shows ads related to this profile. Others try to collect all the information possible about the user, for example e-mail, home address, credit card numbers and online identities (web mails, online-game accounts, forum logins). Although spyware can slow down a computer or sometimes even make it crash this is not the intention of those that designed the spyware. A "perfect" spyware would be a program that performs its function without ever being noticed by the user. Most spyware are designed to target computers that use the Windows operating system.

## 2. Background

**Types of Spyware:**

- **Adware:** "Adware is a less threatening sort of program. Adware is similar to spyware, but does not transmit personally identifiable information, or at least the collector promises not to sell it. Instead, aggregated usage information is collected, and sent somewhere on the internet." [3]

- **Spyware:** "Simply, spyware is software that transmits personally identifiable information from your computer to some place in the internet without your knowledge." [3]

- **Browser Hijackers:** "Browser hijackers can take control of user's web browser. They may alter user's browser settings or change user's default home page to point to some other site and they are capable of sending personal information to third-parties. They may not be detected by firewall software as they are capable of appearing as part of Internet Explorer itself. Due to the variety of functions a browser hijacker can possess, it can be categorized as a Trojan."[7]

- **Dialers:** "Generally, this is software that is installed on user's PC that dials a phone number. Some dialers connect to Internet Service Providers (ISPs) and are designed to provide genuine assistance. However, malicious dialers can attempt to connect user to long-distance or toll numbers without informing, resulting in expensive phone bills ".[7]

- **Tracking Cookies:**"Internet browsers write and read cookies which are small text files with small amounts of data (such as web site settings) which are placed onto user's computer by visiting certain web sites. In many cases, cookies provide a benefit to users as they can retain settings for

when they next visit a web site. In some instances, however, cookies are used to consolidate and track user's behaviour across different web sites, providing marketers with information about his/her web browsing habits ".[7]

- **Key Loggers:** " Also known as 'key loggers' or 'keystroke loggers', these are programs that run in the background on end user's computer and are capable of recording every keystroke user make on keyboard. Key loggers can store information, which could very well include personal details and passwords that user have typed into user's computer, such that it can later be retrieved by third-parties ".[7]

**How does spyware get installed on the end user's Computer? :**

Spyware is installed on the end user's computer in several different ways. Most are installed through an action taken by the user by clicking on a popup or installing another program that has the spyware bundled into the install. The most common ways the user is convinced into installing spyware are listed here below.

1. **Piggybacked software installation:** There are some software applications that will install spyware as part of their install. The fact that the spyware will be installed is often stated in the license agreement the user accepts before installing. This is the case with Kazaa [9] that actually also states on their homepage what bundled software will be installed. Other programs will rely on the fact that a lot of users probably just accept the license agreement without reading it and even if they read it the language used is usually very hard to understand. .

2. **Drive by download:** Drive by download is an attempt by a website to automatically install spyware on the user's computer. Usually this will just produce a security warning stating that the site has tried to execute some code and asking the user to accept that the code is run. If the user has lowered the security level of the browser there might not even be a popup asking if the code about to be run should be trusted.

3. **Browser add-ons:** "Web browser add-ons give different functionality to your Web browser to make browsing a little more fun or effective. Extra toolbars, animated mouse pointers, and stock tickers are all examples of browser add-ons." [8] "Add-ons are typically fine to use, but sometimes they slow down your computer or force Internet Explorer to shut down unexpectedly. This can happen if the add-on was poorly built or created for an earlier version of Internet Explorer. In some cases, an add-on may be tracking your Web surfing habits." [8] In short they are sometimes nothing more than small hidden spyware themselves.

4. **Masquerading as anti-spyware:** This trick plays on the users fear by claiming to be able to remove spyware and protect the user from unwanted programs. When the program is installed it will most likely reassure the user that the computer is free of spyware and then install its own spyware.

## 3. Evaluation Criteria:

**This is the layout for the comparison:**

1. **General:** Some general description and observations of the anti-spyware program.

2. **Installation:** A description of the installation process. This will be very brief unless the tested program has an installation process with choices that is hard to understand.

3. **Detection Capability:** The techniques used by the tested program to find spyware.

4. **Online Updates:** The update procedure of the tested program.

5. **Real Time Protection:** If the tested program has real time protection, this section will contain a test of how well it works.

6. **Popups and alerts:** Screenshots of popups from the different programs (if any). This will contain how the anti-spyware programs react to spyware being installed on the system. This paragraph is only relevant to those programs that have an active anti-spyware agent running on the system.

7. **Full system scan:** This will be one of the major parts in the report. Here will be lots of screenshots showing the steps that need to be taken to do a system scan and what kind of help the user gets when making decisions about what to do with found spyware. Since some of the programs in the test do not have active agents this will be the main section for those.

8. **Performance:** The time it takes to do a full system scan.

9. **Help and manuals:** A description of how helpful the help pages in the program actually are.

10. **Extra features:** This will be a brief discussion of any extra features that is relevant or helpful.

11. **Spycar test:** See below for information about the Spycar test.

**Test setup and method:**
The test is performed on a clean install of Windows that has been fully updated. All tests will be done on the same install since there is not enough time to reinstall the computer between the tests. Partly because of this we will not test what spyware is found by the different programs except for what is blocked by the runtime protection. The main focus for the manual scanning is how easy it is to use and how much help the user gets when making decisions about what to do with the scan result.

We have selected an online testing site, www.spycar.org as a "bad" website to surf to and installing Kazaa for testing installation of bad programs.

**Spycar:** Spycar is a tool that mimics as a spyware, it is designed simply to measure whether user's anti-spyware tool can block or detect the change. Furthermore, Spycar includes a scorebot/clean-up application that tells user how well user's anti-spyware tool defended user, and automatically undoes every alteration made by Spycar and remembers, these alterations are all there, and will not impact the way user's machine works. [1]

**Tests performed by Spy car**
Spycar performs 17 different tests associated with autostart programs, Internet Explorer configuration changes, and network setting changes. All spycar tests focus on Windows machines. [1]

### Autostart Tests

**1. HKCU_Run: "**Spycar try to drop a file and installs a Registry key to execute it under HKLM\Software\Microsoft\Windows\CurrentVersion\Run" [1]

**2. HKCU_Run Once: "**Spycar try to drop a file and install a Registry key to execute it under HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce" [1]

**3. HKCU_Run OnceEx:** "Spycar try to drop a file and install a Registry key to execute it under HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx" [1]

**4. HKLM_Run: "**Spycar try to drop a file and install a Registry key to execute it under HKCU\Software\Microsoft\Windows\CurrentVersion\Run" [1]

**5. HKLM_Run Once:** "Spycar try to drop a file and install a Registry key to execute it under HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce" [1]

**6. HKLM_Run OnceEx:** "Spycar try to drop a file and install a Registry key to execute it under HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx" [1]

### Internet Explorer Config Change Tests

**7. IE-Home Page Lock:** "Spycar try to lock out users from changing the default home page in IE." [1]

**8. IE-Kill Advanced Tab:** "Spycar try to remove the Advanced Tab in user's IE Internet Options Screen." [1]

**9. IE-Kill Connections Tab:** "Spycar try to remove the Connections Tab in user's IE Internet Options Screen." [1]

**10. IE-Kill Content Tab: "**Spycar try to remove the Content Tab in user's IE Internet Options Screen." [1]

**11. IE-Kill General Tab:** "Spycar try to remove the General Tab in user's IE Internet Options Screen." [1]

**12. IE-Kill Privacy Tab: "**Spycar try to remove the Privacy Tab in user's IE Internet Options Screen." [1]

**13. IE-Kill Programs Tab:** "Spycar try to remove the Programs Tab in user's IE Internet Options Screen." [1]

**14. IE-Kill Security Tab: "**Spycar try to remove the Security Tab in user's IE Internet Options Screen." [1]

**15. IE-Set Home Page: "**Spycar try to change user's default home page in IE." [1]

**16. IE-Set Search Page:** "Spycar try to change user's default search page in IE." [1]

**Network Config Change Tests**

**17. AlterHostsFile:** Spycar try to add an entry to user's hosts file (typically c:\windows\system32\drivers\etc\hosts). [1]

## Results:

The spycar test will produce an output file stating how well the anti-spyware defended the user. The result will contain one of three types of result for every test. The three types of result is explained below.

**1. Spycar change allowed:** This means that spycar was able to perform the change on the computer.
**2. Spycar change blocked:** This means that the changes attempted by spycar was detected and removed by the anti-spyware..
**3. Spycar test not performed:** This means that either the test was not run or the test was blocked before it was executed on the computer.

## System Used for Tests:

**Operating System:** Windows XP Professional servicepack2 (fully updated)
**Browser:** Internet Explorer (the spycar only tests Internet Explorer as some spyware come from ActiveX and only Internet Explorer supports this)
**Hardware:** AMD 1800+ with 256Mb of RAM (The only computer we were willing to sacrifice for this test since installing spyware over there is no guarantee user get rid of it all)

**Tested Anti-Spyware Programs:**

These are the 5 products which we have selected and test these on the above mentioned criteria.

1. Ad aware (free version)
2. Spybot Search and destroy (freeware)
3. Windows Defender(free if the user has a valid Windows license)
4. Spyware Doctor (limited version)
5. Spycatcher Express (freeware)

## Tested Systems:

## 1. Ad aware Personal (free)

1. **General**
   Ad aware personal is a free anti-spyware scanner from Lavasoft. The program supports on demand scanning but does not have the real time protection offered in the commercial (free) versions.

2. **Installation:**
   Installation of this program is easy and straightforward with no other choices to be made than where to install and for what type of users.

3. **Detection Capability:**
   Ad aware uses mostly known signatures to detect threats but claims to be able to find even threats that are similar to those already known [2].

4. **Online Updates:** At first startup a *popup* asks if the anti-spyware definitions should be updated to the latest version. After that updates are made by pressing the update button in the main screen. If the definitions are older than a set threshold Ad aware will produce a reminder to update the definitions. One can set how many days can pass before the definitions are considered outdated.

5. **Real Time Protection**
   Real time protection is only available in the commercial version of Ad-Aware and has not been tested.

6. **Popups and alerts:**
   Since the tested version of Ad-Aware does not include real time protection there are only popups produced in the full system scan and descriptions of these have thus been included in that section.

7. **Full system scan:**
   A scan is performed by clicking the ”Scan now“ button in the *main window.* This opens the *scan screen* where the type of scan wanted is be selected. The most interesting for normal use is the smart system scan and the full system scan. One thing that is confusing is that the green and red marker labeled ”Search for negligible threats“ and ”Search for low-risk threats“ are actually buttons to activate/deactivate these options. After selecting the type of scan to perform the *scanning screen* is opened. Clicking

the next button will bring up the *scan results* screen and clicking the show log file button will also bring up the scan results but with the scan log tab open. The programs listed in the scan results are what are found after installing Kazaa and then performing a full system scan. All threats found that are not considered negligible are listed as critical objects. Note that critical objects include everything from tracking cookies to trojans. To get rid of the threats found the checkbox for the threats should be marked and then the next button should be pressed. Clicking quarantine will put the selected threats in quarantine and clicking next will bring up a *popup* stating that the threats have been removed. The reason for having the quarantine button is for when files are to be put into quarantine and the default action of clicking next is to just remove them.

8. **Performance:**
   Doing a full system scan on the test system took 3 minutes 4 seconds which is the fastest full scan in the test.

9. **Help and manuals:**
   Help with deciding what to do with found spyware comes in the form of an information window that is accessed from the right click menu under the critical objects tab. Selecting this will bring up the object details window for that object.

10. **Spycar Result:**
    For this test to be relevant to our test program a full system scan was performed after running all of the spycar tests. This is not really reflecting reality since users will most likely not run a scan every time they have used the Internet. The result from this test without the scan is obviously that nothing is blocked since the program never checks for any problems. We can see that even though there is no runtime protection Ad aware still managed to find and remove some of the changes made by spycar.

## 2. Spybot Search & destroy (freeware)

1. **General**
   Spybot search & destroy is a free anti-spyware scanner from www.spybot.info. The program is a pure on demand scanner with some extra features for automatically configuring Internet Explorer to block known bad sites and programs.

2. **Installation:**
   Installation of Spybot search & destroy is easy and straightforward. Worth noting is that the user will get a *popup* at the end of the install. During the first startup the program will ask if a *register backup* should be made and then *checks for* and *downloads* updates.

3. **Detection Capability:**
   Spybot search & destroy uses known signatures to detect spyware and claims to have ”ways to generically detect malware mutations“. [3]

4. **Online Updates:** Updates are made by clicking the ”Search for updates“ button in the *main window***.**

5. **Real Time Protection** Spybot search & destroy does not have any real time protection in the form of an active agent.

6. **Popups and alerts:**
   Since there is no runtime protection there are hardly any popups to be evaluated. The only ones that occur are during a full system scan.

7. **Full system scan:**
   A full system scan is performed by clicking the “Check for problems”-button in the *main window***.** Doing this brings up the *search screen* in which the found threats will be displayed when the scan is completed. To get rid of these spyware simply press the “Fix selected problems”-button. Here we have found that some of the programs that are to be removed are loaded into memory and cannot be removed directly. Spybot search & destroy then produces a *popup* asking if a scan should be performed on reboot. Doing this will start Spybot and run the scan before any other programs are loaded. After selecting an appropriate action *another popup* confirms the choices made. Now the scan screen is shown again with the removed spyware clearly marked with a green check mark and the spyware still in the system (but that are to be removed on reboot) unmarked.

8. **Performance:**
   Doing a full system scan with Spybot search & destroy took 11 minutes 30 seconds.

9. **Help and manuals:**
   Clicking on any found threat in the scan result window will show some information about that threat. The amount of information available is varying from threat to threat. Description of *Altnet* and the description of *CommonName vary a lot.*

10. **Extra features:**
    Spybot search & destroy has a feature called *immunize* that, when activated will tweak Internet Explorer to block installing known spyware. As mentioned this only works for Internet Explorer and blocks installers through their ActiveX IDs

11. **Spycar Result:**
    As with Ad-Aware a full system scan was performed after running the spycar test. The test result of this not so realistic test**,** and we have seen that Spybot search & destroy did not stop any of the test cases presented in the spycar test.

## 3. Windows Defender (free with a valid Windows license):

1. **General:**
   Windows defender is an anti-spyware program from Microsoft that is free if the user has a valid Windows license. The program supports both on demand scanning and has a real time agent.

2. **Installation:**
   Installing Windows Defender has a few extra steps compared to the other software in this test. The software requires validation of Windows before the program can download and *then again* when the install program is started. After getting the file and starting the install *there* is the only choice for the user. The last window of the install has a choice to update and run a quick scan.

3. **Detection Capability:**
   Trying to find out what principle Windows Defender uses to identify threats have not been fruitful and the testers must admit that we do not know how Windows Defender detects threats.

4. **Online Updates:** Windows defender can be set to run scheduled scans and to download new definitions before each scan.

5. **Real Time Protection:** Windows defender has a running agent that provides real time protection. Defender can be set to notify about changes in the system from different sources. When a change is made by a known process a message is presented that Windows Defender detected certain changes.

6. **Popups and alerts:**
   Windows defender has a few kinds of popups and alerts. For changes in the system made by know programs a small *notification* is shown just to alert the user that something has happened. When something that is classified as a potentially unwanted program a popup is presented and when something classified as a program that might compromise the user's privacy or computer another popup is presented. The difference is that potentially unwanted programs are displayed with a yellow header and potentially dangerous programs are displayed with a red header. When installing Kazaa the two types of popups were displayed simultaneously. If the same option is not wanted for all the threats found there is an option to press the review button. Here an action to be performed for each threat can be selected. If more information is needed there is a link at the bottom of each description to a more detailed online documentation. One thing that seems cumbersome is that whenever a detected threat is removed a popup is displayed stating that the system needs to be restarted for Defender to protect the system.

7. **Full system scan:**
   A full system scan is performed by pressing the little arrow next to scan and choosing full scan. When the scan is completed a result window like will appear. After this clicking on the "review items detected by scanning" the *same screen* as pressing review from the runtime detection popup opens.

8. **Performance:**
   Running a full system scan with Windows defender took 14 minutes and 19 seconds on our test system.

9. **Help and manuals:**
   The amount of help available to the user for making a decision is pretty good. In the *review screen* there is a lot of information available with

links to even more information should it be needed.

10. **Spycar Result:**
    Since Windows Defender has an online protection agent the spycar test was performed as it should be with just the runtime protection stopping the test programs. The result is very good with only one change allowed. As was noted in the popups and alerts we are prompted to restart our system after choosing to remove an attempted install by spycar. Since the test includes 17 different subtests and a restart was required after most of them we did what any normal user would do after a while, we chose to restart later just moving on.

## 4. Spyware Doctor (limited version)

1. **General**
   Spyware doctor has a free version and a commercial version. The difference is that the free version includes runtime protection but does not include the ability to remove threats after manual scans. There is also a third option of getting a limited version of the program as a part of the Google pack. This version has the ability to remove found threats but has some limitations in the runtime protection. The Google pack version was used for the tests with the motivation that any user installing an anti-spyware would want to remove found threats. To get a grasp on what the difference in performance would be in the spycar test both the Google pack version and the free version was submitted to this test.

2. **Installation:**
   Installation of the software is easy and straight forward. After the install the definitions database is automatically updated and a scan is performed.

3. **Detection Capability:**
   Spyware doctor uses a combination of known signatures and heuristics to detect spyware [5]

4. **Online Updates:** To update the spyware definitions select the smart update button from the main window.

5. **Real Time Protection:** Note: according to the Spydoctor webpage [5] the Google pack version has some limitations in the functionality of the real time protection.

6. While trying to install Kazaa with the real time protection active a lot of the components in the install was blocked. In fact so many components were blocked that Kazaa was unable to install and an error message stated that the install file should be downloaded again before attempting to reinstall. To be able to run the full system scan test with Kazaa installed the online protection had to be disabled during the install**.** In the disable screen there is several options for disabling the protection for different periods of time.

7. **Popups and alerts:**
   Spyware doctor has one type of popup for alerting the user that something potentially unwanted is trying to install itself on the computer. Every threat that is being blocked is presented in a new popup and these popups can fill the screen pretty fast when several threats are blocked in a short period of time. When a few threats are blocked at once the popups start filling up on the screen and when a lot of threats are blocked at once the alerts were just piling up on top of each other in the upper right corner of the screen.

8. **Full system scan:**
   A full system scan is performed by choosing the ”Full Scan“ option from the ”Start Scan” tab in the main window. This will scan the computer and show the scan results page. Getting rid of the found threats is done by marking the ones that should be fixed and pressing the Fix checked button. Doing this on the spyware installed by Kazaa will produce a popup alerting to the fact that removing some programs listed as spyware might break the license agreement accepted when installing the host program. After removing the threats the scan summary shows some information of the scan and actions taken. Also a popup alerts to the fact that a reboot is required for the complete removal of the spyware.

9. **Performance:**
   A complete system scan with Spyware doctor took 9 minutes and 57 seconds on our test system.

10. **Help and manuals:**
    The runtime protection blocks all spyware-

classed actions to the system with just an alert to the fact that it happened so no help is needed there. For the threats found with a full system scan there is some information about what the detected threat does in the system.

11. **Spycar Result:**
    Even though the tested version of Spyware doctor does not have the full runtime protection we tested the software using only this. The result is not looking good, not a single one of the test cases was blocked. Because this was such a bad result the free version with the full runtime protection was tested too, this did however give the same result.

## 5. Spycatcher Express (freeware)

1. **General**
   Spycatcher express is a lighter version of the Spycatcher anti-spyware program from Tenebril. Spyware express has both runtime protection and on demand scanner.

2. **Installation:**
   Installing Spycatcher express is pretty straight forward though the install requires a valid e-mail to continue the installation. After providing one and completing the install procedure the Spycatcher configuration wizard starts. Here the latest definitions are downloaded and installed, then a scan is performed. After this Spycatcher ask if it should remove tracking cookies during scans and if spyware reports, information about found spyware not yet classified, should be sent to Spycatcher to help improve the software. Lastly the option to create a schedule for scanning the computer is presented.

3. **Detection Capability:**
   Spycatcher express uses profiles, behavioral analysis and contextual intelligence [6] to detect spyware.

4. **Online Updates:**
   Online updates are performed by pressing the ”Update Now“ button under the updates menu**.** The automatic update option is only available in the paid version of Spycatcher.

5. **Real Time Protection:** The tested version of Spycatcher express has full real time protection. While trying to install Kazaa a lot of the components needed for the install were blocked resulting in Kazaa being unable to install. To be able to run the full scan test the real time protection had to be turned off from the protection menu while Kazaa was installed.

6. **Popups and alerts:**
   Spycatcher only has one type of alert. The alert is not informative at all just stating that it prevented spyware from running.

7. **Full system scan:**
   To perform a full system scan the ”Deep Scan“ option should be chosen from the “spyware scan menu”**.** This will scan the computer and produce a scan information page with information of detected threats and what has been done with them. Pressing the next button will open the “application actions” page saying what spyware has been found and what action that was taken for that spyware. If a file is not recognized by Spycatcher but is suspicious, the user gets to choose what to do about the file. Any new spyware found after the initial scan will just be added to the list of found spyware on the computer. Even if the option remove is chosen the spyware files are still in the ”My spyware” window. The program says that the files are being removed in the background but no indication is given as to when or if the files are actually deleted. A new scan will result in no new threats being detected and then the same screen with all the spyware ever found on the computer with the option of what to do with them is presented.

8. **Performance:**
   A full system scan with Spycatcher express took 3 minutes and 12 seconds on our test system making it the second fastest software in the test.

9. **Help and manuals:**
   Clicking on any found threat in the “my spyware” window will bring up a webpage with the information of the found threat. This webpage also includes user comments on the treats. These comments can sometimes give hints of what to do with some strange file found by Spycatcher when there is no official information. Marking a treat and clicking the traces button will bring up a window with where the file identified as a threat was found and any other files associated with it.

10. **Spycar Result:**
    There actually is no result for the spycar test of Spycatcher express since the runtime protection blocked the test programs before they even had a chance to run. This leads to that the scoring program refusing to run since it could not detect that a test had been performed.

## 4. Suggestions

Install anti-spyware software that has real time protection like Spycatcher Express or Spyware doctor to avoid getting the problems into the computer in the first place.

Try to avoid different activities that are mentioned in the section “How does spyware get installed on the end user's Computer?”

Read the installation list of any software from sources that is not fully trusted carefully. Make sure there are no extra programs are being installed.

Do full scans regularly, preferably with different software than the one providing the real time protection.

Turn off ActiveX in Internet Explorer and only activate it when absolutely needed. For example when updating Windows.

## 5. Conclusions

After installing and testing these anti-spyware softwares, Spycatcher has the best results as it blocks all the attacks made from spycar before they are executed on the machine. This good blocking has some downsides too though. Spycatchers way of finding spyware during scans yields some false positives that might make the user remove files that are needed for the system to run as intended.

The second best in the spycar test was Windows Defender with only one change allowed. This would make the software really good if it weren’t for the fact that a reboot is required after every threat that is blocked.

Ad aware came in third in the spycar test but this was after a manual scan was performed. Since the user will most likely not perform a manual scan several times a day the result only shows what kind of changes *could* be detected.

From the tests we conclude that the security provided by anti-spyware does not depend only on if it has real time protection but also on what methods is used to detect spyware.

Another thing to notice is that since the anti-spyware softwares use various databases and techniques when identifying spyware, doing a scan with more than one software might fix a larger part of the changes made by spyware.

Since we found that getting rid of spyware can be a long process (some of the programs are really hard to get rid of) sometimes the user might need to consider reinstalling the computer. This should in our opinion be done regularly anyway and doing this will make absolutely sure that there are no spyware still hiding somewhere on the computer.

## 6. References


**[1]. www.spycar.org**

**[2]. www.lavasoft.com**

**[3]. www.spybot.info**

**[4]. www.microsoft.com/athome/security/spyware/software/default.mspx**

**[5]. www.pctools.com**

**[6]. www.tenebril.com**

**[7]. http://www.pctools.com/mrc/glossary/**

**[8]. http://www.microsoft.com/windowsxp/using/web/sp2_addonmanager.mspx**

**[9]. www.kazaa.com**