Comparing Anti-Spyware Products – a Different Approach

M.Saqib and M.Papadaki

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Spyware is one of the biggest emerging threats that can target both home users and organisations simultaneously. Lots of Anti-Spyware products are available in the market which can protect from Spyware threat. Existing research shows that Spyware causes financial loss and efforts are being made to test Spyware to propose the best Anti-Spyware products to the end users. This research focuses on different aspects of Anti-Spyware testing that the test should be conducted in real life environment in which the users operate. Anti-Spyware programs are selected by carefully researching through existing test results conducted by different internet security companies. The products are evaluated and tested to propose the suitable products to the end users. Some recommendations are also proposed on the basis of this research to help end user to increase their Spyware security.

Keywords

Spyware, Security, Anti-Spyware, Internet

1 Introduction

Spyware is a type of potentially unwanted programs (PUP) (Antispyware Coalition, 2007) becoming the significant problem for most computer users. Spyware tracks and monitors the user activities (Erbschloe, 2005), particularly browsing habits, typing of credit cards and passwords (McFedries, 2005), whether online or offline (Good et al., 2005) and share the user information with the third party companies for advertising and other targeted marketing purpose. Mostly it affects the system performance (Wu et al., 2006, Schmidt and Arnett, 2005) and stability and slows down the internet connectivity. There are many people involved in developing, distributing and benefiting from the Spyware itself. These include hackers, developers, distributers, online advertising companies, investing people and sponsors (Payton, 2006).

2 Spyware Threats

The word "Spyware" was first used on 16 October 1996, in a humorous post about Microsoft's business model (Wienbar, 2004) which appeared on Usenet (News, 2007, Lavasoft AB, 2007) but in 2000 the term was used in press release for Zone Alarm Personal Firewall (Wienbar, 2004). According to a report that first Spyware was spread through a game called "Elf Bowling" in 1999 (News, 2007).

In 2007, Spyware caused damaged to the 850,000 computers alone in USA, which made people to replace their computers (Consumer Reports, 2007). Due to lack of knowledge and expertise in this field, most of the people did not know how to resolve this problem. Gartner IT Summit 2006 estimates that over the next two years, Spyware will affect 20% to 50% of enterprises. And by the end of 2008 less than half of the organizations will affected by Spyware (Gartner, 2006).

One in seven of the worst security breaches involved Spyware (DTI, 2006) which gives a clear indication that Spyware is one of the biggest threats to the users. Different Anti-Spyware vendors show top ten threats on their websites which are periodically collected from the users.

Web root	Computer Associates	Threat Expert
Trojan-Downloader-Zlob	Trymedia	SpyAxe/Zlob
Trojan.Gen	Nuvens	Virtumonde/ErrorSafe/WinFi
Trojan-Ace-X	Estalive	xer
Trojan-Agent.Gen	HotBar	FakeAlert
Trojan Downloader Matcash	New.Net.Domain.Plugin	Lop.com
Trojan Agent Winlogonhook		PurityScan
2nd-thought		Maxifile
Trojan-Relayer-Areses		SpySheriff/SpywareNo
Trojan-Poolsv		Zango/180Solutions/Hotbar
Trojan-Phisher-Bzub		Seekmo
		ISTBar

Table 1: Top ten Spyware threats (Webroot Software, 2008, CA, 2008, PC Tools, 2008)

3 Creation of Spyware – Latest trends

Spyware has gone through many changes throughout its history. But still the main aim of creating the Spyware is to steal private and secret information (Erbschloe, 2005). In the past attackers have been trying to create false applications, browser toolbars and tracking cookies to collect personal information and behaviours (Wu et al., 2006). There are quite a few techniques used in developing of Spyware like manipulating the system calls, using DLL files and configuration settings. Randomising the file names and storing it in different locations is also a technique used in Spyware development (Wu et al., 2006).

Attackers are creating deceiving applications like multimedia players and rogue applications to trick the user to install the Spyware. One of the examples of this type of Spyware is Viewpoint media player (SpywareInfo, 2005). With the increase use of web 2.0 and social networking websites like myspace.com and orku.com and blog website, attackers are now targeting these areas. Two examples of website being compromised in 2007 are Salesforce.com and Monster.com. In one of the report at "Webmaster World" that 75% of the Google's BlogSpot are spam (McAfee, 2008). Another way is Steganography (Westphal, 2003), which hides messages or steeled personal information in images or multimedia contents like (audio, video), when an attacker steals the information then using this technique he hides the information into image and send to the server as an attachment (Kessler, 2004, Dunbar, 2002).

Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet (Dunbar, 2002).

4 Anti-Spyware Products Comparison

There are numbers of anti Spyware products available in the market. Various methodologies are available for Anti-Spyware testing. Few of them have been highlighted in this research.

4.1 Existing Research

Installing the threats on a computer and testing it with different Anti-Spyware scanners is one of the approaches used by newspapers and magazines to rate and review the Anti-Spyware products (AV-Test, 2008, PC Magazine, 2008). Sometimes the system is tested only with a newly operating system installed with security patches such as Windows (CNET Networks, 2006b) and then the system is bombarded with Spyware. These types of tests are also used to track the performance of the system before and after the Spyware are installed on the computer (Arnett and Schmidt, 2005).

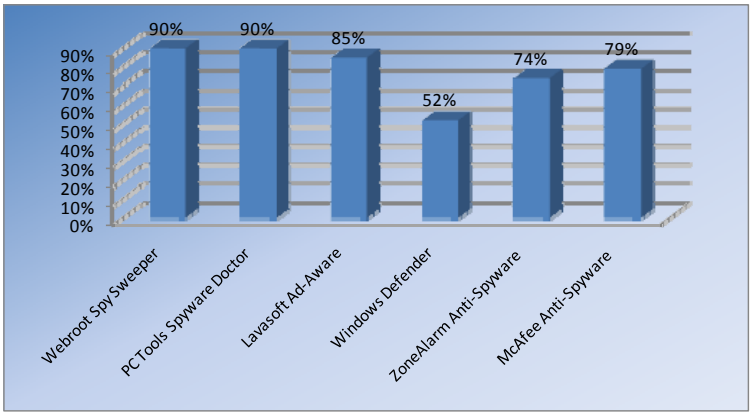

Figure 1: AV-Test - Spyware Detection Rate (CNET Networks, 2006a, PC Magazine, 2008, AV-Test, 2008)

Similarly at 2Spyware.com, they take the image of a computer which was being used by a novice user and tests that image every time (JSC "Elektroniniai sprendimai", 2008). The computer is used by the novice user for approximately two weeks before it is being put into the action. The approach is quite good for comparison purpose but in our research only one PC was available and it was not possible to take the image of the whole computer and reload it every time the test was being performed.

Top IT magazines like PC Magazine, PC World, CNET Reviews, Consumer Research website and AV-Test Testing performs Anti-Spyware testing. The tests were conducted by PC magazine and PC World and CNET, the test cases and Spyware threats data provided by German Research Company (AV-Test.org) which conducts virus and Spyware research and testing. The tests were then conducted at

CNET labs (CNET Networks, 2006b) and PC Word testing labs specially created for software testing.

The graphs below shows the detection rate for specific Spyware threats like registry keys and browser helper objects. Results show that Anti-Spyware mostly detects and removes BOHs (Browser Helper Objects) as compared to the removal of registry keys. Registry keys removed by all the programs are at the lower rate for all the security programs. Webroot Spy Sweeper and McAfee Anti-Spyware removes 100% of the browser helper objects and could remove 88% and 79% of the registry keys respectively.

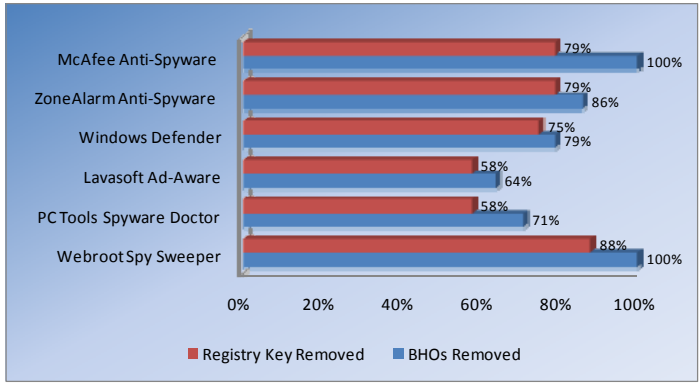

Figure 2: Specific Spyware Detection Rate (CNET Networks, 2006a, PC Magazine, 2008)

4.2 Products Selection

There are numbers of Anti-Spyware products available in the market, but to compare all of the products is a long process and is out of scope of the research. The products selected for the comparison are based on the top ten Anti-Spyware products selected by the renowned magazines and newspapers including PC World, CNET and ConsumerSearch. All the selected products are listed amongst the top ten charts of these magazines and they are highly rated by the consumers too.

In total there are seven products selected, and the selected products is a mix of Anti-Spyware scanners and Anti-Spyware as a part of whole internet security system. Here is the complete list of Anti-Spyware programmes which were selected in the research.

1. Webroot Spy Sweeper
2. PC Tools Spyware Doctor
3. Lavasoft Ad-Ware
4. Windows Defender
5. ZoneAlarm Anti-Spyware combined with the firewall suite
6. Norton Anti-Spyware combined with internet security suite
7. McAfee Anti-Spyware while combined with complete suite

4.3 Research Methodology

The approach taken in this research was quite simple and straight forward. The tests were conducted on the system one by one, and there was no priority for any application. The computer was being used regularly as a normal computer is being used. But the usage was kept limited just to make sure that new applications and Spyware are not installed during the testing process. Anti-Spyware was installed one by one so that they may not interfere with each other. Each of the Anti-Spyware was fully updated with the latest program updates and Spyware signatures.

During the testing phase most of the efforts were put to scan the whole computer system and do not go for real-time protection. This is because in real-time protection the Anti-Spyware scanner removes the threats without asking the user what to do. Sometimes the Spyware hides itself if there is a new installation or there is a new Anti-Spyware programmed installed on the system. So this leaves less Spyware for the next Anti-Spyware program to detect properly

The tests were performed on a computer with Processor type: Intel(R) Core(TM) 2 CPU T5500 @ 1.66GHz, Total Physical Memory: 1.0 GB and Total Disk Space: 120 GB. Operating system was Windows XP with service pack 3 installed and all the updated patches installed.

4.4 Anti-Spyware Testing

All the programs were tested and evaluated according to the research methodology explained above. Every Anti-Spyware program was first updated to get the most up-to-date information about the program like how many Spyware it can detect, what is the update date and version etc. And then the product was tested by scanning the whole computer system by using the default features turned on in the product.

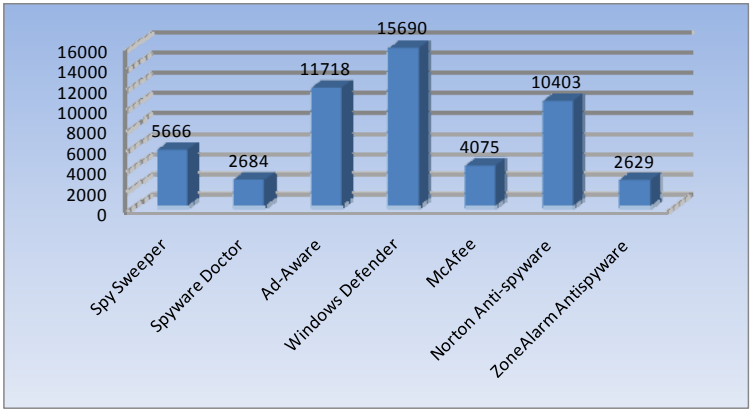

Figure 3: Spyware Scanning Rate

Windows Defender scans 15,690 files per minutes which is very high rate as the average scan rate for all the Anti-Spyware program is 7,552 files per minute. The slowest scanner was ZoneAlarm Anti-Spyware with 2,629 files per minute. LavaSoft's Ad-Aware was also amongst the fastest scanners with 11,717 files per

minute. One may argue that the faster scanner may not be scanning the whole file, instead it scans the starting bytes and ending bytes of each file and then forwards to the next file. Whereas the slower scanner may scans the whole file including its contents and header. But for the end user it does not matter whether a program scans the whole file or part of a file, the point is the protections against Spyware threats.

The most important effectiveness and efficiency measure is the numbers of threats a scanner can find. But again it can be argued that what is a threat and what is not a threat. For example tracking cookies are sometimes considered low level threats and sometimes not considered a threat because they can be removed easily by the internet browser. Some people argue that a tracking cookie cannot be a threat, as it can be removed manually without any expertise needed (Microsoft, 2008).

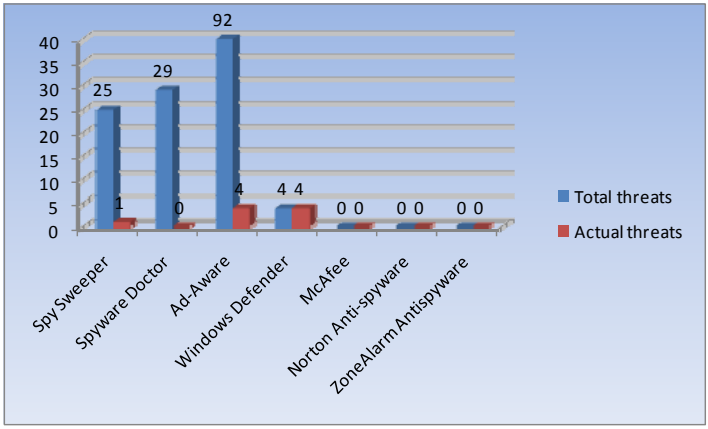

Figure 4: Total vs. Actual Threats Detected

Numbers of Spyware threats detected during the test are being summarised in the above chart. Maximum numbers of threats were 92 detected by Ad-Aware, and surprisingly McAfee, Norton and ZoneAlarm Anti-Spyware programs did not detect even a single Spyware program or a tracking cookie. So program with lots of extra features like antivirus, firewall or any blocking features might cause the scanner to slow down and reduce its effectiveness.

5 Conclusion

Options are available to the end user about the selection of the desired Anti-Spyware product. User can select to install a free program and compromise on certain features like real-time protection and customised scans. Anti-Spyware comes as a part of the complete security suit which fulfils all the needs in one single program. Again some compromise on customisations options and effectiveness. More features mean more chances that the Spyware could not be detected as the program is designed to detect and remove various types of threats, and there is not enough expertise available in the program to do all the tasks accurately. Standalone Anti-Spyware programs are available for complete Spyware protection, which can detect and remove any type of Spyware either cookies or key logger. Again there is a compromise on system

resources and memory usage. So user has lots of options available and can choose the best possible option which suits the needs and performs the tasks as desired.

6 References

Antispyware Coalition, (2007). Definitions and Supporting Documents, Anti-spyware Coalition. Retrieved January 02, 2008 from http://www.antispywarecoalition.org/documents/2007definitions.htm

Arnett, K. P. and Schmidt, M. B., (2005). Busting the ghost in the machine. Commun. ACM, Vol. 48, Iss. 8, p. 92-95.

AV-Test, (2008). Anti-virus comparison test of current anti-malware products, Ziff Davis Publishing Holdings Inc. Retrieved May 28, 2008 from http://blogs.pcmag.com/securitywatch/Results-2008q1.htm

CA, (2008). Internet Security Outlook, Computer Associates. Retrieved January 10, 2008 from http://ca.com/files/SecurityAdvisorNews/ca_security_2008_white_paper_final.pdf

CNET Networks, Inc, (2006a). CNET top 10 antispyware apps, CNET Networks, Inc. Retrieved January 12, 2008 from http://review.zdnet.com/4520-3688_16-6456087-1.html

CNET Networks, Inc, (2006b). How we test: Antispyware software, CNET Networks, Inc. Retrieved July 12, 2008 from http://reviews.cnet.com/Labs/4520-6603_7-6719061-1.html

Consumer Reports, (2007). Net Threats - State of the Net 2007, Consumers Union of U.S., Inc. Retrieved June 12, 2008 from http://www.consumerreports.org/cro/electronics-computers/computers/internet-and-other-services/net-threats-9-07/overview/0709_net_ov.htm

DTI, (2006). Information Security Breaches Survey 2006, Department of Trade and Industry. Retrieved January 04, 2008 from http://www.berr.gov.uk/files/file28343.pdf

Dunbar, B., (2002). A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment, SANS Institute. Retrieved June 05, 2008 from http://www.sans.org/reading_room/whitepapers/covert/677.php

Erbschloe, M., (2005). Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code. Burlington: Elsevier Butterworth-Heinemann. 232.

Gartner, Inc, (2006). Information Technology Summit. London United Kingdom: Gartner Inc

Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D. and Konstan, J., (2005). Stopping spyware at the gate: a user study of privacy, notice and spyware. Proceedings of the 2005 symposium on Usable privacy and security. Pittsburgh, Pennsylvania, ACM

JSC "Elektroniniai sprendimai", (2008). Anti-spyware comparison, July 10, 2008 from http://www.2-spyware.com/compare.php

Kessler, G. C., (2004). An Overview of Steganography for the Computer Forensics Examiner Forensic Science Communications, Vol. 6, Iss. 3, p. 23.

Lavasoft AB, (2007). The History of Spyware, Lavasoft. Retrieved January 02, 2008 from http://www.lavasoftusa.com/support/spywareeducationcenter/spyware_history.php

McAfee, Inc, (2008). Top 10 Threat Predictions for 2008, McAfee Advert Labs. Retrieved January 20, 2008 from http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_avert_predictions_2008.pdf

McFedries, P., (2005). Technically Speaking: The Spyware Nightmare. IEEE Spectrum, Vol. 42, Iss. 8, p. 72-72.

Microsoft, Inc, (2008). Windows Defender, Microsoft Corporation. Retrieved May 15, 2008 from http://www.microsoft.com/windows/products/winfamily/defender/default.mspx

News, P. S., (2007). Chapter 2: History of Spyware, PC Security News. Retrieved January 02, 2008 from http://www.pcsecuritynews.com/spyware_history.html

Payton, A. M., (2006). A review of spyware campaigns and strategies to combat them. Proceedings of the 3rd annual conference on Information security curriculum development. Kennesaw, Georgia, ACM

PC Magazine, (2008). Antispyware - Reviews and Price comparisons from PC Magazine, Ziff Davis Publishing Holdings Inc. Retrieved June 16, 2008 from http://www.pcmag.com/category2/0,2806,1639157,00.asp

PC Tools, (2008). Spyware Doctor - Best Spyware Removal, May 15, 2008 from http://www.pctools.com/spyware-doctor/

Schmidt, M. B. and Arnett, K. P., (2005). Spyware: a little knowledge is a wonderful thing. Commun. ACM, Vol. 48, Iss. 8, p. 67-70.

SpywareInfo, (2005). Spyware Weekly Newsletter, SpywareInfo.com. Retrieved January 15, 2008 from http://www.spywareinfo.com/newsletter/archives/2005/nov4.php#viewpoint

Webroot Software, Inc, (2008). Webroot spy sweeper, Webroot Software, Inc. Retrieved May 08, 2008 from http://www.webroot.com/En_US/consumer-products-spysweeper.html

Westphal, K., (2003). Steganography Revealed, SecurityFocus. Retrieved January 10, 2008 from http://www.securityfocus.com/infocus/1684

Wienbar, S., (2004). The spyware inferno, News.com. Retrieved January 06, 2008 from http://news.cnet.com/2010-1032-5307831.html

Wu, M.-W., Huang, Y., Wang, Y.-M. and Kuo, S.-Y., (2006). A Stateful Approach to Spyware Detection and Removal. Proceedings of the 12th Pacific Rim International Symposium on Dependable Computing. IEEE Computer Society