ASSESSMENT OF ANTI SPYWARE TOOLS FOR SIGNATURE AND BEHAVIOR BASE TECHNIQUES

Nabeel Alam Khattak[1], Dave Chadwick[2], Riaz Ahmed Bhatti[1], Shafqat Ali Shad[1], Faisal Shafique Butt[1], Ehsan Ullah Munir[1]

Department of Computer Science, COMSATS Institute of Information Technology, Wah Cantt, Pakistan[1].
School of Computing and Mathematical Sciences, University of Greenwich, London, UK[2]
nabeelalamkhattak@hotmail.com, D.R.Chadwick@gre.ac.uk, riazahmad_200@yahoo.com, shafqat@ciitwah.edu.pk,
faisalshafique@yahoo.com, ehsanmunir@gmail.com

ABSTRACT: *In the modern computational world spyware became evident whether its personal computers or business units. Intention of this research paper is to do critical analysis of spy-wares and techniques used by anti spy-wares. From this paper a user can easily understand what is spyware and how it effect the user system. From this paper the user will also identify "how it works?". This paper will also show the user how to compare the best tool and where to find the anti spyware?*

INTRODUCTION

A spy-ware is a software through which the people steal personal information of the user without his knowledge [15]. Some Internet technologies and delivery methods to the third person are known collectively as spyware. Many of spywares are legal, free and can inflict havoc on the best-laid technology programs and plans. It is hard to define what is spyware, what does it do, and how can user prevent it from affecting his educational and organization's operations? In general term spyware describes a collection of technologies that help external parties in "gathering information about a person or organization without their knowledge and concern." Further more to the minor annoyances spyware generates, redirected pages, redirected searches, and pop-up ads. The infection of spyware can have more spiteful effects which includes the gathering of personal information from unwitting users his e-mail addresses, credit card numbers, and even passwords. There are some spywares that has the ability to read the files on the user's hard drive and track the strokes which user makes on his keyboard. This type of spyware can even track the use of other applications, like chat rooms. Finally, the infection of spyware can lead to slow Internet connections[3,8].

Many big media companies that offer them to place banner adds in their product in exchange for portion of the revenue from banner sales. Through this way you do not pay for the software, the software developer or web developer they are only paid for it. If the user find the banner infuriating then there is usually an option to remove them by paying them a regular licensing fee[14].

It is generally a software that internet user download often without knowing. This software collect data and then transmit the user data to help marketer advertise to them more effectively. The issue of privacy become more important, when more people are getting connected to the internet. Today there are some techniques that were originally created to provide sensible functionality which are being misused to monitor the activity of the user. The example of such techniques are web browsers, cookies, HTTP refers and HTML source tag.[15,16]

Background

Spy ware has long history. Many people worked on spyware. They first define and then derived its form and classes. They thought that spyware only steal the information but after some practical work they came to know that it transfer the information to the third party. Spy-ware was compare with has been described as the irritation of the internet and said to be a big threat to the internet users(Ward & Roselli, Sipior). The merchant of spy-ware defend their application by claiming that they provide a valuable service for consumers and by providing the advertising software which is paid and premium content (Zengo,2006) in exchange for view targeted advertising. But problem is that the business model for software distribution often encourages wrong or illegal activity[5,7,].

Now a days deferent kinds of spyware and one hundred of such programs exist .These programs are due to rapid development in technology. As compare to old period spyware is relatively new phenomenon of the computer. However there is no exact definition of the term "spyware" which is typically used to refer to a category of software that from a user's perspective and stealthily gathers information about a use of computer and relays that information send back to a third party[1,16].

Spy-ware is different from other types of mal-ware such as virus and worms. The aim of spy-ware is not to cause the damage to other system generally and also not to spread to other system. Instead it steals the personal information such as keystroke, browsing pattern and it also monitor the behavior of the user. First it gets the information and sent it back to the distributor of spy-ware. A large number of anti-spyware products in the market online. The aim of these product to identify and then remove spy-ware from the system of the users [9,13,18]. Spy-ware programs are dangerous, and can harm "the privacy & security" of user. Credit card, debit card, bank details, pin no etc are comes in privacy issues while in security terms of spywares, for examples Trojan horses, mal-wares, cookies, browsing hijacking, key-loggers, web bugs etc. To overcome these threats, there are some anti-spyware tools such as Spy-doctor, Spybot and McAfee .

These tools are using some techniques to detect spywares. Such techniques are behavior based and signature based[11].

METHODOLOGY

In this report by using comparison methodology to find the best tool in terms of their test results, features available and cost analysis. For this methodology, focusing on three products of anti-spyware these are based on above mention techniques. These three tools are spyware Doctor, 'Spy-bot Search and Destroy' and McAfee.

Test Comparison Methodology:

In the test comparison methodology, a test environment was set up on a computer system to show the overall performance of these antispyware tools. The test environment consisted of

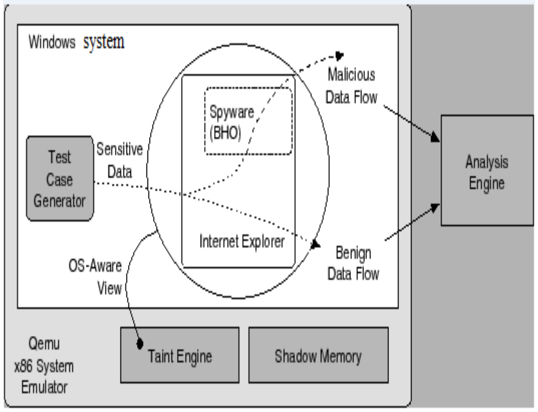
By design this methodology for the cost assessment of different Anti-Spyware tools on the basis of their using techniques to detect the spywares on the system. For this purpose, by making set a test environment on computer system with following specification:

Computer Name: Home
User Name: NABEEL
Operating System: Microsoft Windows

The above mention system is stand alone PC connected with wireless network at home, and it is being used for all tests of anti-spyware tools. The reason for defining this methodology is to find the best tool which generate best results on different systems and secure them from the current threats of spywares, malwares, adware and different malicious codes.

Behavioral Based Anti-Spyware:

Many security sellers in the answer make addition of activity jamming to their anti spy-ware solution in the reaction to the restrain of signature-base technology. A activity jamming technology has not the ability to familiar with a threat given by its code, rather by its action. This is very much important application level supervision. It is difficult to make a difference between non constructive and constructive behavior in the limit though supremacy behavior-base spyware exposure. It is too much difficult and tough for IT Administrators to make standard behavior-base security policies and procedure which precisely identify spy-ware throughout the organization. This is the reason that security policies and procedures are made with behavior base solutions and this tend to be very relax or some time restrict[12].



For analyzation of BHO(browser helper object) it is first installed on the guest OS(operating system). Then launch the internet explorer and loading the BHO component on the startup. Also started the test generator. The test generator's task is to imitate a surfing user by replaying a previously recorded browsing session. When the sensitive data such as a URL(Uniform Resource Locator) that test generator navigates to enters the internet explorer process then it is marked as tainted. From tainted point engine tracks how the information is processed by the browser and BHO. To be able to distinguish between actions taken by the internet explorer and those by the BHO, the tainted engine differentiates between code that is executed by the Internet Explorer and code run on behalf of the BHO. The taint engine also monitors when (and where) tainted data exits the address space of the browser. When the Internet Explorer writes out tainted data because of regular browser activity, the flow is recorded as benign. When tainted information leaks because of activity on behalf of the BHO, the information flow is recorded as malicious. In this case, the analysis engine classifies the BHO as spyware.[18]

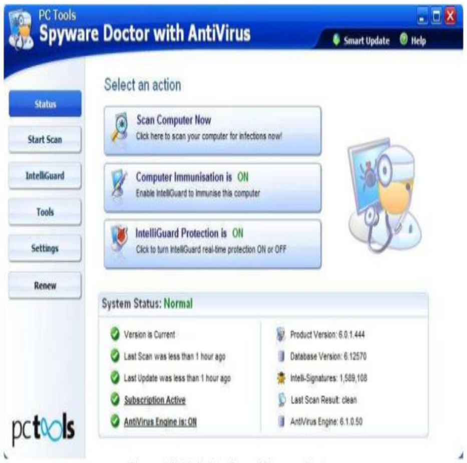
"Behavioral based anti-spyware technique an abstract characterization of the behavior of most of the spyware programs that rely on the Internet explorer Browser Helper Object (BHO) and toolbar interfaces to monitor the user's browsing behavior." For test comparison first choose behavioral based technique Anti-Spyware tool called "Spyware doctor".

Doctor" that published by PC Tools.

Full version information:
Version: 6.0.1.44
File size: 23,877KB
Release Date: 9 June, 2009.
Operating System: Window Vista SP1& windows XP

Protection against: spyware, Adware, Spyware Trojans, key-loggers, Identity Theft, Hijackers, Tracking Threats, Rouge Anti-Spywares, Unwanted Software, Phishing, Pop-ups and bad websites.

After successful installation and doing updates following screen shows for Spyware doctor[10].



Select an action

Scan Computer Now
Click here to scan your computer for infections now!

Computer Immunisation is ON
Enable IntelliGuard to immunise this computer

IntelliGuard Protection is ON
Click to turn IntelliGuard real-time protection ON or OFF

System Status: Normal

- Version is Current
- Last Scan was less than 1 hour ago
- Last Update was less than 1 hour ago
- Subscription Active
- AntiVirus Engine is: ON

Product Version: 6.0.1.444
Database Version: 6.12570
Intelli-Signatures: 1,589,108
Last Scan Result: clean
AntiVirus Engine: 6.1.0.50

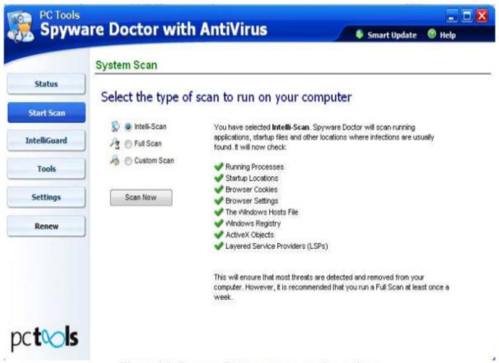
Figure 1.0: Main Interface of Spyware Doctor

Figure 1.0: Main Interface of Spyware Doctor

Figure 1.0 illustrate Spyware Doctor main interface that includes Features on left side that will describe in detail in features comparison section. Body section includes some actions and System Status Information that change on the basis of test results, database version, installed signatures and the user subscription. Spyware Doctor give three types of option to scan the system,

but its Intelli-scan option is used for scanning because it uses behavior based technique and blocks both known and unknown spyware threats before they are installed and give real time protection against malicious behavior involving spyware, track cookies, malicious active X objects, browser hijacker, key-loggers, Trojans and more as

shown on below figure 1.1.



Select the type of scan to run on your computer

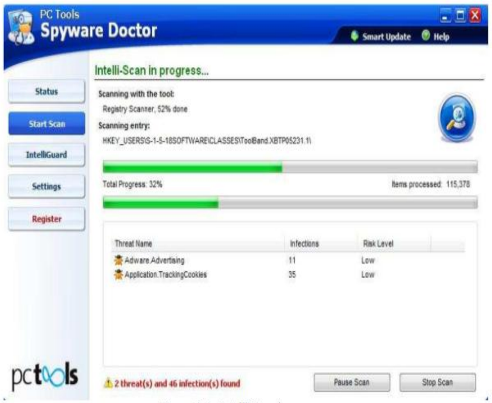
You have selected **Intelli-Scan**. Spyware Doctor will scan running applications, startup files and other locations where infections are usually found. It will now check:

- ✓ Running Processes
- ✓ Startup Locations
- ✓ Browser Cookies
- ✓ Browser Settings
- ✓ The Windows Hosts File
- ✓ Windows Registry
- ✓ ActiveX Objects
- ✓ Layered Service Providers (LSPs)

This will ensure that most threats are detected and removed from your computer. However, it is recommended that you run a Full Scan at least once a week.

Figure 1.1: Spyware Doctor system scanning options

After this Intelli Scanning on system was performed to find different spyware . It is shown in figure 1.2 .



Scanning with the tool:
Registry Scanner, 52% done

Scanning entry:
HKEY_USERS\S-1-5-18SOFTWARE\CLASSES\ToolBand.XBTP05231.1\

Total Progress: 32%

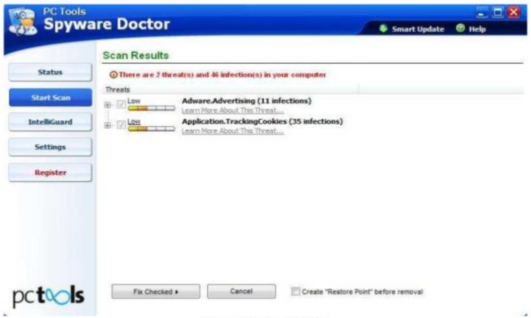
Items processed: 115,378

Threat Name	Infections	Risk Level
Adware.Advertising	11	Low
Application.TrackingCookies	35	Low

⚠ 2 threat(s) and 46 infection(s) found

Figure 1.2: Intelli-Scan in progress

Finally the results showed two threads and forty six infections on the system,, this test result can be seen from the figure 1.3 as below



There are 2 threat(s) and 46 infection(s) in your computer

☑ Low Adware.Advertising (11 infections)

☑ Low Application.TrackingCookies (35 infections)

□ Create "Restore Point" before removal

Figure 1.3: Scan Results

Signature Based Anti-Spyware:

"Identify known spyware instance by comparing the binary image of these programs with a number of uniquely characterizing signature called signature based technique."

For second test, signature based technique Anti-Spyware tool called "Spybot- Search and Destroy" was used that is published by Safer Networking Limited copyright 2000-2008.

Full version information:

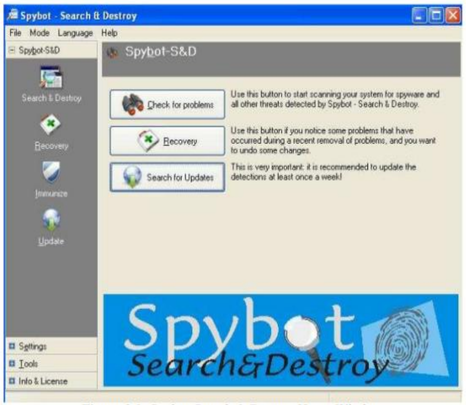
Version: 1.6.2.46

File size: 15,600KB

Operating System: Microsoft Window, Linux/Unix,

Protection against: Adware, BHO (Browser Help Object), Browser Hijacker, Dialer, Key-loggers, Malware, Spyware, Trojans, Worms and PUPS (Possibly Unpopular Software)[9].

After successful installation on the home system and performing updates shown following figure.



Use this button to start scanning your system for spyware and all other threats detected by Spybot - Search & Destroy.

Use this button if you notice some problems that have occurred during a recent removal of problems, and you want to undo some changes.

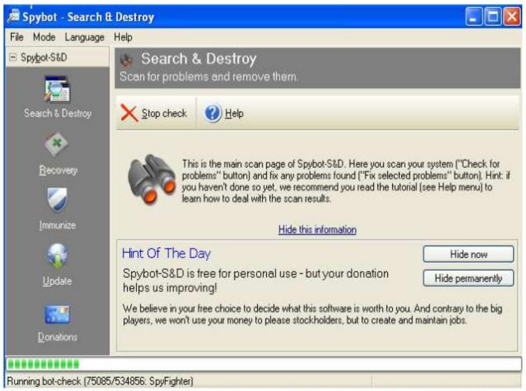
This is very important: it is recommended to update the detections at least once a week!

Figure 2.0: Spybot-Search & Destroy Home Window

Figure 2.0 illustrate Spy-bot-Destroy & Search main interface that includes features of the product on left side that will describe in detail in features comparison section. Body section includes three basic action of spy-bot that is Check for Problems (Used for system scanning and destroy threats), Recovery and Search for updates.

Start Scanning:

By pressing check for problem button, spy-bot start doing scanning of whole computer system by using signature technique, in which every file has been matched with the updated database of spywares codes.



Scan for problems and remove them.

This is the main scan page of Spybot-S&D. Here you scan your system ("Check for problems" button) and fix any problems found ("Fix selected problems" button). Hint: if you haven't done so yet, we recommend you read the tutorial (see Help menu) to learn how to deal with the scan results.

Spybot-S&D is free for personal use - but your donation helps us improving!

We believe in your free choice to decide what this software is worth to you. And contrary to the big players, we won't use your money to please stockholders, but to create and maintain jobs.

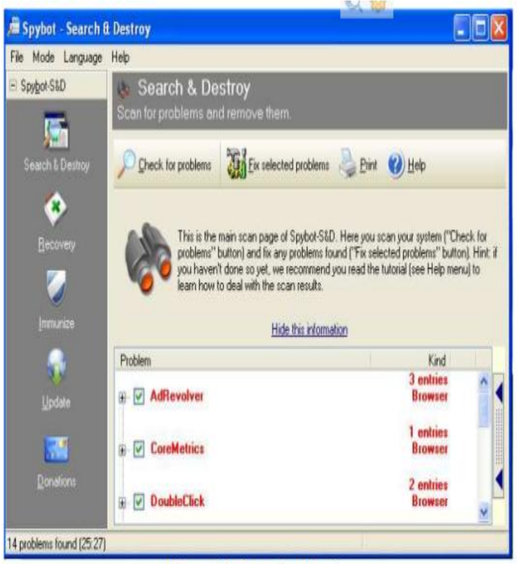
Running bot-check (75085/534856: SpyFighter)

Figure 2.1: Spybot scanning in progress using signature based technique

SCAN RESULTS:

After completing the scanning process spy-bot identified fourteen problems that is actually less then behavioral based technique.

Image 2.2 shows the results and problems that are identified.



This is the main scan page of Spybot-S&D. Here you scan your system ("Check for problems" button) and fix any problems found ("Fix selected problems" button). Hint: if you haven't done so yet, we recommend you read the tutorial (see Help menu) to learn how to deal with the scan results.

Problem	Kind
☑ AdRevolver	3 entries Browser
☑ CoreMetrics	1 entries Browser
☑ DoubleClick	2 entries Browser

14 problems found (25:27)

Figure 2.2: Scanning Results

Anti-Spyware based on both above Techniques:

For third test, another Anti-spyware and Anti –Virus tool called "McAfee-Security Centre" was use.It uses signature based and behavioral based approaches. Reason of using McAfee for third test is same to check the results of the test that how strongly it attacks on the spywares and viruses.

Full version information that I used for my test is:

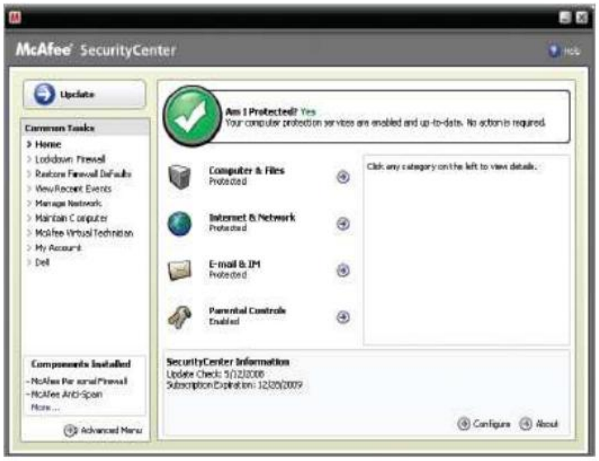
Version: 2.0.148.0

File size: 821KB

Operating System: Microsoft Windows

Protection against: Virus, Malwares, Adware, BHO (Browser Help Object), Browser Hijacker, Dialer, Key-loggers, Spyware, Trojans, Worms and PUPS (Possibly Unpopular Software)[11].

After successful installation on the home system and performing updates shown following figure.



Am I Protected? Yes
Your computer protection services are enabled and up-to-date. No action is required.

Computer & Files: Protected
Internet & Network: Protected
E-mail & IM: Protected
Parental Controls: Enabled

Click any category on the left to view details.

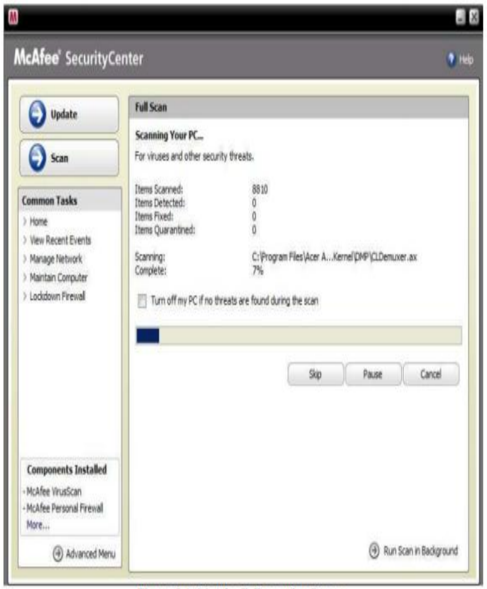
SecurityCenter Information
Update Check: 5/12/2008
Subscription Expiration: 12/20/2009

Figure 3.0: McAfee security center Home Window

On the left hand side Tools and Features shown for McAfee Security Center and main body indicated Protection status on the basis of Computer and files scan protection, Internet and network protection, E-mail & IM protection and Personal control enabling.

Start Scanning:

By pressing scan button, McAfee give two options for scanning Full computer Scan and Quick Scan. After selecting full System Scanning it start crunching whole system and process shown in figure 3.1.



Full Scan

Scanning Your PC...
For viruses and other security threats.

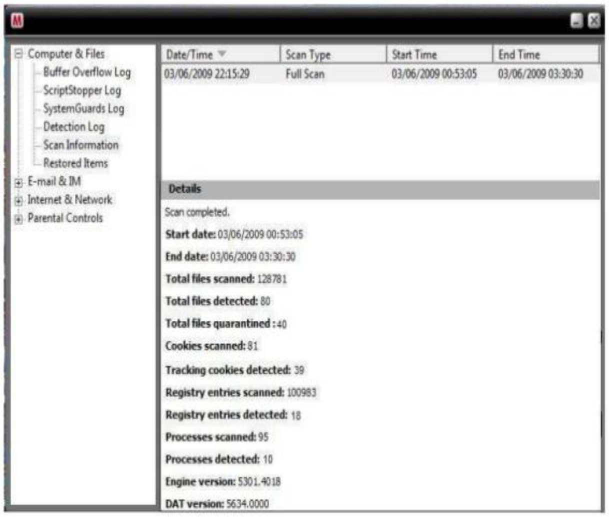
```
Items Scanned:      8810
Items Detected:     0
Items Fixed:        0
Items Quarantined:  0

Scanning:           C:\Program Files\Acer A...Kernel\DMP\CLDemuxer.ax
Complete:           7%
```

□ Turn off my PC if no threats are found during the scan

Figure 3.1: McAfee Full scanning Process

SCAN RESULTS:

After completing the scanning process McAfee generate following results on the basis of both signature and behavior technique.



Date/Time	Scan Type	Start Time	End Time
03/06/2009 22:15:29	Full Scan	03/06/2009 00:53:05	03/06/2009 03:30:30

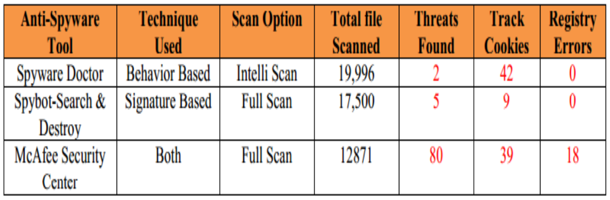
Details

Scan completed.
Start date: 03/06/2009 00:53:05
End date: 03/06/2009 03:30:30
Total files scanned: 128781
Total files detected: 80
Total files quarantined : 40
Cookies scanned: 81
Tracking cookies detected: 39
Registry entries scanned: 100983
Registry entries detected: 18
Processes scanned: 95
Processes detected: 10
Engine version: 5301.4018
DAT version: 5634.0000

Figure 3.2:McAfee Scan Result

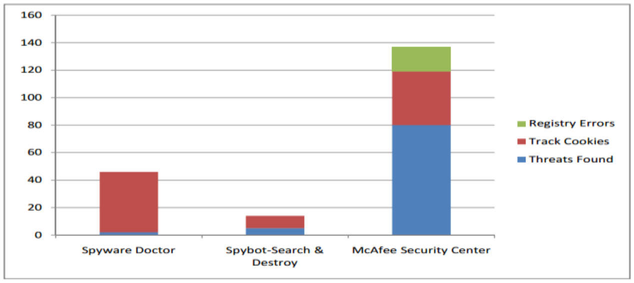
Test Results Comparison:

Table 1.1: Test Result Comparison



Anti-Spyware Tool	Technique Used	Scan Option	Total file Scanned	Threats Found	Track Cookies	Registry Errors
Spyware Doctor	Behavior Based	Intelli Scan	19,996	2	42	0
Spybot-Search & Destroy	Signature Based	Full Scan	17,500	5	9	0
McAfee Security Center	Both	Full Scan	12871	80	39	18

From Table 1.0 shows comparison result. Spy-Doctor while scanning use behavior base technique . It scanned 19,996 files and 2 threats, 42 Cookies, and no registry errors found. The spy-bot search & destroy used signature base technique and found 5 threats, 9 cookies, and no registry errors, after scanning of 17,500 file. McAfee used both signature and behavior base technique, through this technique after scan of 12,871 files it found 80 threats,39 cookies and 18 registry errors.



Graph 1.0: Test Result Comparison

The graph 1.0 shows the comparison of test result . In this graph it shows that McAfee Security Center is the best with the Spy-ware Doctor and Spy-Bot Search & Destroy.

Features Comparison Table:

Table 1.2: Feature Comparison

McAfee	Spy-Doctor	Spy-bot
Protection from Virus and Malicious Attacks.	Malicious attack controlled plus Active-X blocker and Trojan Detector.	Included Anti-spyware, Anti-virus, Anti-adware.
Firewall Protection	Intelli-Guard for Malware protection and key logger removal	Unique feature: Removal of Dialers
Anti-spyware and Anti-Virus included	Intelli-Scan feature enables to kill threat in 3 minutes	Removal of key loggers and Trojans
Anti-phishing included	Detect and remove Root-kit threats and Removal of Complex threats	Removal of tracking cookies
In-depth coding analyses		Backup of Removal Programs

From Table 1.2_shows feature comparison. From this comparison user can easily understand which is better and which is not. As per my I got result from this table is McAfee having best features rather then Spy-Doctor and Spy-Bot.

Cost Benefit Analysis:

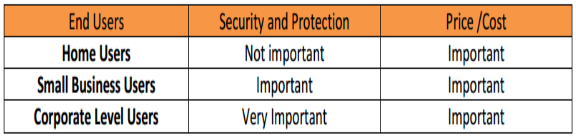
Cost benefit analysis defined as weighting total cost expected against the total benefits expected of one or more options available for the best and profitable option. In term of anti-spyware tools and using techniques, cost benefit analysis is defined as "Choosing the best product by the benefits and security it provide against the expected cost".

For doing this three type of end users were considered,

1. Home user
2. Small Business Users
3. Corporate Level users

For the end users it always depends what are the benefits and in which cost it will be? It either be not important, Important or very Important as mention in below table:

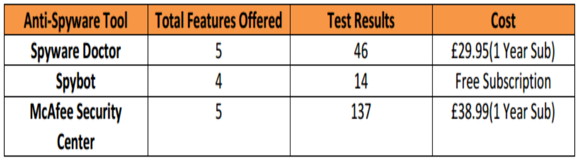
Table 1.3: Cost Benefit Analysis



End Users	Security and Protection	Price /Cost
Home Users	Not important	Important
Small Business Users	Important	Important
Corporate Level Users	Very Important	Important

For the cost benefit analysis for three different anti-spyware tools based on two techniques. following table shows the best product choose by the end user.

Table 1.3: Cost Analysis



Anti-Spyware Tool	Total Features Offered	Test Results	Cost
Spyware Doctor	5	46	£29.95(1 Year Sub)
Spybot	4	14	Free Subscription
McAfee Security Center	5	137	£38.99(1 Year Sub)

Cost of the product also different from single pc to multi computers and it also depends on which level of protection need by the end user.

RECOMMENDATIONS

On the basis of test results, feature and cost analysis following recommendations are made.

For Home or Basic User:

It is recommended that home users used Spy-bot for to protect their system from different type of spyware attacks. Because it is free of cost in subscription and based on signature based technique which is automatically updating itself when connect. And provide security and protection with no cost.

For Small Business Users:

For small or medium level users it is recommended that they will use Spyware Doctor for the protection of their assets from different spyware attacks. Reason behind is that Good behavior based protection with advance Intelli scan system and other good feature of embedded virus protection as well. It generates log files for individual users and also provides root kit for high threats. Cost is not much high as compared to the security and protection it provided, so it affordable for small business users.

For Corporate Level Users:

At corporate level, security is very matter for the effective operations of their business so they must consider high protection against the cost.

For the corporate level users it is recommended that they used McAfee Security Center for the better protection in very relevant price. Other Features like firewall protection and virus scan also give more security and satisfaction to the users.

REFERENCES

1) Boldt, M. (2007). Privacy-invasive software. Karlskrona: Blekinge Institute of Technology.
2) Cordees, C. (2005). Monsters in the closet: Spyware awareness and prevention (2nd ed., pp. 23-56). Educause Quarterly.
3) Cordess, C. (2004). Monsters in the closet: Measures for Spyware awareness and prevention (2nd ed.).
4) Eisenhauer, M. (2005). 6th annual institute on privacy law. New York, NY: Practising Law Institute.
5) Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., & Konstan, J. (2005). Stopping spyware at the gate: a user study of privacy, notice and spyware, 43--52.
6) Gutzman, C., Sweep, S., & Tambo, A. (2003). Differences and similarities of spyware and adware. University Of Minnesota Morris.
7) Hu, Q., & Dinev, T. (2005). Is spyware an internet nuisance or public menace?. Communications Of The ACM, 48(8), 61--66.
8) Kirda, E., Kruegel, C., Banks, G., Vigna, G., & Kemmerer, R. (2006). Behavior-based Spyware Detection., 6.
9) Majoras, D. (2006). Remarks of ... on "finding the solutions to fight spyware. Washington, DC: U.S. FTC.
10) Mcafee. Operating Systems, Supports Windows XP SP2/SP3, Vista SP1/SP2, Windows 7 and Windows 8, System Requirement: Internet connection, 256MB RAM or higher, Minimum 20 MB of free disk space, Browsers: Microsoft Internet Explorer 7.0 or later: Mozilla Firefox version 3.6 or later. (2014).
11) (2014). Retrieved 22 October 2014, from Spybot - Search & Destroy - CNET Download.com http://download.cnet.com/Spybot-Search-Destroy/3000-8022_4-10122137.html#ixzz2U5N7nrBu
12) Moshchuk, A., Bragin, T., Gribble, S., & Levy, H. (2006). A Crawler-based Study of Spyware in the Web.
13) Raitt, D. (2007). World Wide Web applications in South Africa. [Bradford, England]: Emerald.
14) Saroiu, S., Gribble, S., & Levy, H. (2004). Measurement and Analysis of Spyware in a University Environment., 141--153.
15) Spyware Doctor, License type: Shareware (Version Spyware Doctor 6.1.0.2898). (2014).
16) Wang, Y., Roussev, R., Verbowski, C., Johnson, A., Wu, M., Huang, Y., & Kuo, S. (2004). Gatekeeper: Monitoring Auto-Start Extensibility Points (ASEPs) for Spyware Management., **4**, 33--46.
17) Weinshall, D. (2006). Cognitive authentication schemes safe against spyware, **6**, 40-96