Comparing Anti-Spyware Products

W.Martins and S.M.Furnell

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

Abstract

Spyware has been more of a threat to the home user than other malicious software for the motive behind its creation which has been the tracking of the user and his activities on the Internet alongside the stealing of his personal or confidential information. As a result of this threat, various anti-malware products have been introduced to remove spyware from home PCs. This research examines the effectiveness of present day anti-malware products in removing spyware from a test computer. The results suggest that the removal capabilities of the products are unsatisfactory and indicate there are compelling reasons for more thorough detection and removal of spyware from home computers.

Keywords

ASEPs, Anti-Virus, Registry Keys, Spyware.

1 Introduction

For the computer user, the Internet is an increasingly dangerous place by the day. Where once all a user had to fear was the threat of viruses, present day trends paint a more sombre picture of an amalgamation of adware, worms, viruses, Trojans, spyware, and root kits the home computer is at risk of encountering once connected to the Internet. In an age in which increasing amounts of personal and confidential information is being stored on the home computer, the preponderance of malware on the Internet harbours significant risks. This growth in malware threats and the corresponding shift, by malware authors, from “ego trips” to pecuniary motives portends a significant risk of loss of trust in the Internet with potential damaging implications for e-commerce in particular.

Numerous studies however indicate the pace of malware prevalence and subsequent infection of home computers is on the increase. A 2008 Internet security study by Webroot (2008) for instance, reported a 500% increase in web borne malware compared to 2007 alongside another study estimating the infection of 35 million computers each month by malware (Pandalabs 2009). It is in this environment fraught with risks the computer user navigates.

Though, as earlier mentioned, user awareness of computer security is on the increase (F-Secure 2009), studies have repeatedly indicated security awareness and knowledge is still lacking, even among advanced users (Furnell et al. 2007). Additionally, while it has been a standard security recommendation for users to

avoid adult and 'warez' websites of which users are at greater risk of malware infection, there is compelling evidence that users are still at risk of infection when they visit legitimate websites (BBC 2009). Home computers are adjudged to be at greater risk of infection compared to corporate computers as a result of user habit to use their computers whilst logged in as administrators and the administrative restrictions enforceable on corporate computers are absent in home computers. It is in light of these short-comings, greater emphasis is placed on the ability of anti-malware products in protecting the home user from the menace of malware. This paper details a research undertaken to investigate the effectiveness of present day anti-virus products in removing spyware from a computer.

2 Methodology

2.1 Test Bed Preparation

For the test, Windows XP service pack 3 was installed on a system along with Microsoft Office 2003 and Adobe reader. All operating system and application updates were subsequently installed. To confirm all updates had been applied, the vulnerability tools - Microsoft baseline security analyser (MBSA) and Secunia personal software inspector - were run against the system. Additionally, the system was scanned with an anti-virus program which was later removed.

2.2 Anti-virus Product Selection

Due to the fact that most standalone anti-spyware products have been integrated into anti-virus products, anti-virus programs were downloaded from various anti-malware vendor websites. The list of anti-virus vendors was obtained from the Microsoft site (2008). The anti-virus products selected are as presented below:

Anti-Virus Products	Version
Eset NOD32	4.0.437.0
F-Secure	9.00 build 149
Kaspersky	6.0.3.837
Malwarebytes	1.39
Panda	9.00.00
Sophos	7.6.10
Vipre	3.1.2775
Webroot	6.1.0.128

Table 1: List of Anti-Virus Products Selected

2.3 Test Tools

For the successful conduct of any test involving malware, tools are required to monitor and record the creation of files and registry keys by the program and to monitor the state of the system prior to spyware infection and after spyware removal.

To accomplish this objective, a collection of freeware and shareware system utilities, comprising registry and file monitoring tools, were adopted for the study. The tools were selected based on a track record of implementation in malware forensic analysis and incident response (Aquilina et al, 2008) and various Internet sources. Malware has been known to compromise the integrity of system utilities. To ensure the integrity of the tools selected would not be compromised by the spyware programs during the course of the study, a MD5 hash was taken of all tools before the installation of the spyware samples and then compared with another MD5 hash after installation.

Additionally, tools of similar functionality were selected. This was for a variety of reasons. Paramount was a bid to ensure result consistency and integrity. For instance, in a scenario in which a single tool is adopted, the integrity of any results obtained is based on the assumption that the program correctly captured or interpreted the required data. In the circumstance where the data capture process or interpretation is suspect, the integrity of the study is put to question. Secondly, the strengths of a single tool may be restricted in certain areas of operation and unable to provide a comprehensive overview as required.

The selected tools are as follows:

- **Autoruns**: A startup program monitor. Used to display which programs are configured to run during system bootup or login.
- **Regshot**: A freeware system comparison tool. Used to compare the changes to the registry and file system prior to and after the installation of a program.
- **Regsnap**: A shareware system comparison tool. Also offers the same functionality as Regshot.
- **InstallWatch**: Used to track system changes as a result of program installations.
- **Hijackthis:** Used to generate an in depth report of the registry.
- **Pstools**: A collection of command-line utilities used to monitor the processes running on a system.
- **Process monitor**: A system monitoring tool. Used to view real-time registry and file/process activity on a system.
- **Process Explorer**: Utility used to list the processes running on a system and the handles and dynamic link libraries (DLLs) loaded.
- **R-Drive Image**: A disk imaging tool. Used to create disk images for the study.
- **Rootkit revealer**: A rootkit detection utility.

2.4 Sample Selection and Installation

Spyware is installed in a system in a variety of ways among which are through drive-by downloads when users visit infected websites, through spyware bundled with free or shareware applications, or through the delivery of spyware as a payload of other malware onto a system.

For the test, samples of spyware/adware were identified and collected for the test. A crucial aspect of any malware test is the identification and confirmation of the samples to be used in the test (Antispyware Coalition 2008). Additionally, identified samples should be of a wide variety and appreciable number for statistical relevance (Marx and Morgenstern 2008). The samples used for the test were of various categories: adware, spyware, potentially unwanted programs such as jokes, Trojan-Spy, file sharing tools and rogue anti-malware applications. Overall, the samples were fifty-five in number.

The samples were identified and selected using a number of internet sources such as the malware databases of anti-malware vendors. For instance, the anti-malware, Emsisoft, lists adware/spyware programs along with the websites which host them. Another resource which was utilised was the malwaredomain list site (2009) which lists websites that host malware or exploits.

To reduce the risk that the samples collected contained any other unknown malicious components, the samples were uploaded to the online virus scanner, Virustotal (2009) for confirmation of the authenticity of the samples.

2.5 Test Execution

A snapshot of the system was taken and an image of the system was taken and stored as a master copy. The spyware samples were then installed on the system and the system rebooted so as to ensure full installation. On reboot, a snapshot of the system state was taken and its image saved. This image was used for subsequent comparison tests with various anti-virus products and the two snapshots were compared to determine the files and registry keys created or edited by the spyware programs.

Internet access was enabled during the installation of the samples and disabled afterwards. Spyware when first installed on a system may update its components or download additional components. Internet access was enabled concerning this and disabled shortly afterwards. Internet access was disabled so as to reduce the risk of system inconsistency due to the risk of download of additional malicious components after the snapshots would have been taken. Internet access was subsequently enabled solely for the purposes of anti-virus updates after product installation and disabled afterwards.

Each anti-malware program tested was configured for full scanning and the system was scanned three times. Full scanning was enabled as a result of the various default configurations of anti-malware products. For instance, a vendor may prioritise speed over efficiency in setting default configurations while another may configure the default scan as a full scan. As such, results from a study in which the anti-malware products are tested based on the default configuration are likely to be flawed (Harley and Lee, 2007). Taking this into consideration, full scanning was configured on all the tested anti-malware products. The products were also configured to remove all traces of malware without prompting. In cases where the delete option had to be selected manually, it was chosen. The delete option was selected so as to gauge the success or failure of the products in removing the spyware. The study was undertaken using the default user account, the administrator.

The system was scanned three times by each product to ensure thorough removal of suspected programs. Additionally, the samples were left on the desktop to determine the removal capabilities of the anti-malware program concerning uninstalled spyware.

3 Results and Analysis

Malware when installed into a system places its files in critical areas of the registry and file system. These areas are commonly referred to as the Auto-Start Extensibility Points (ASEPs) (Harriman 2006). The installation of the samples resulted in the creation of registry keys in to these locations as well as in other areas of the registry. As the samples adopted for the purposes of the study were of various types, it was observed that both the spyware and adware programs installed more files when compared to the Trojan-Spy samples which resulted in the creation of few files and registry keys. For instance, one of the spyware programs was observed to create no less than seven registry keys in the ASEPs.

Overall, the installation of all the samples resulted in the creation or modification of critical registry keys and files. Sixty seven registry keys were created along with three hundred and eighty files. The anti-virus program was then installed on the system and run for a total of three times. On completion, a snapshot of the system was taken and then compared with the snapshot of the system taken after the installation of the samples. The results comparing the effectiveness of the products are displayed in Figure 1.

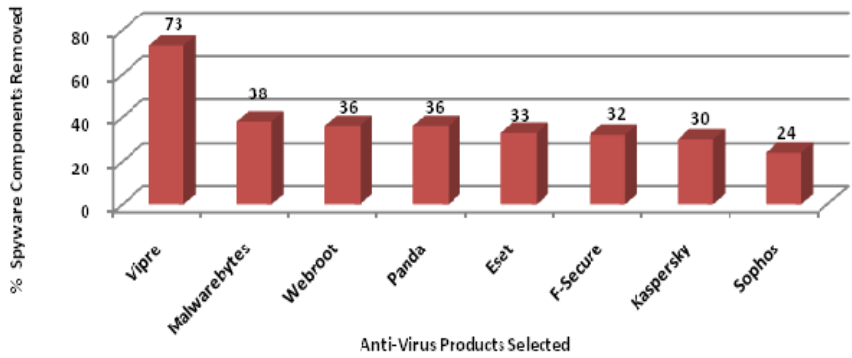

Figure 1: Spyware Components Removed

Anti-virus products are expected to detect and remove malware threats. This is accomplished through the termination of processes and removal of files and registry keys. As shown above, the removal capabilities of the anti-virus products suggests there is room for improvement. The performance of the products was below average, with the exception of the Vipre product which was observed to be the most effective product in the removal of both spyware files and registry keys. Additionally, as depicted in the below Figure 2, the number of processes still active after completion of the tests shows the computer is still at significant risk from malware.

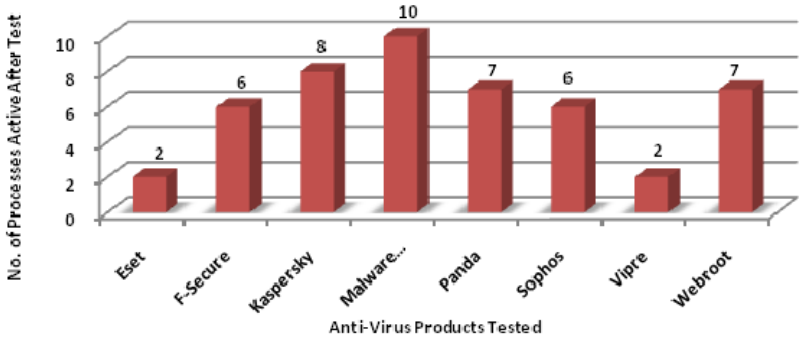

Figure 2: Processes Active after Test Completion

These results raise troubling issues. Foremost, the low rate of removal of spyware components and presence of active spyware processes suggest users are still at risk of spyware. This is particularly worrisome as there are greater expectations on anti-virus products to protect users as most users may not have the required technical expertise or knowledge to supplement the use of anti-malware products. As such, these users may undertake their normal activities on the Internet with a false sense of security.

Additionally, the results indicate the inability to effectively detect the spyware components is not peculiar to one product. This suggests a weakness on the part of the anti-malware industry as a user would still remain unprotected from spyware regardless of the product he were to select.

Further results from the research indicate the removal process of the spyware components are not as thorough as may be expected. As earlier highlighted, anti-virus products are expected to remove all registry keys that are created by spyware or edit the values of the keys if removal would disrupt the legitimate operations of the computer. Figure 3 details the percentage of registry keys which were left intact despite the removal of files associated with the keys.

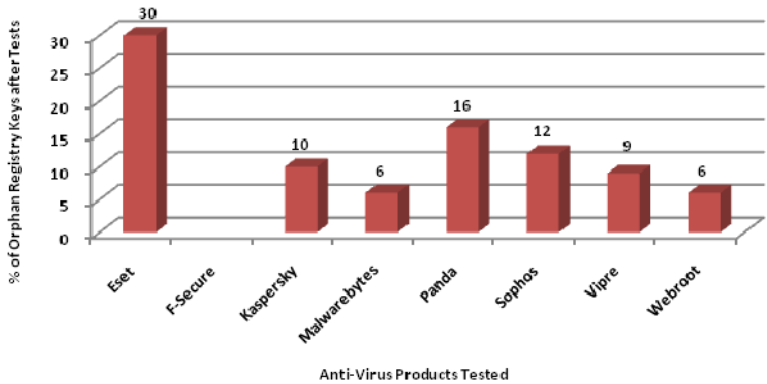

Figure 3: Orphan Registry Keys after Test Completion

As displayed in the above figure, only one anti-virus product ensured no orphan registry keys were left. The prevalence of the orphan registry keys has undesirable implications for both the user and the anti-virus vendor particularly where the keys execute programs automatically on user logon or system startup. For the user, the appearance of error messages on the inability of an application to run on user logon or system startup may cause uncertainty and lead the user to believe that his computer supposedly fixed by an anti-virus product remains faulty. On the other hand, the user may be inclined to believe the anti-malware product was ineffective in the removal of the risks on his computer. In a scenario where the user switches to a different anti-virus product and experiences similar occurrences, there remains the possibility the user may become discontented with the anti-malware industry and subsequently abstain from using the Internet.

4 Conclusion

The importance of anti-virus products for the protection of home computers from malware cannot be over-estimated. Studies have shown users lack the means or knowledge to protect themselves from the threat of malware thus placing substantial responsibility on anti-malware products. The research conducted to examine the effectiveness of present day anti-virus products in removing spyware components from a computer suggests the products may not remove spyware components as may be expected by users. As such, users are still at significant risk of spyware regardless of the anti-virus products selected and may either proceed to browse the Internet under an assumption of false security or desist/limit use of the Internet after experimenting with various products.

The research also suggests anti-virus products may not remove spyware components in a thorough manner as incidences of orphan registry keys were observed to be predominant among the products. The existence of such keys may trigger error messages which may be troubling for users and may result in unintended commercial consequences for anti-malware vendors. Overall, this research has underlined the risk users may still face despite the adoption of anti-malware products.

5 References

Aquilina, J., Casey, E., and Malin, C. (2008) *Malware Forensics: Investigating and Analysing Malicious Code.* Massachusetts: Syngress.

Anti-Malware Testing Standards Organisation (AMTSO) (2008) *the Fundamental Principles of Testing.* Available at: http://www.amtso.org/documents/doc_download/6-amtso-fundamental-principles-of-testing.html (Accessed: 4 January, 2009)

Antispyware Coalition (2008) *Considerations for Anti-virus Product Testing.* Available at: http://www.antispywarecoalition.org/documents/20080417testing.pdf (Accessed: 2 January, 2009)

Autoruns (2009). Available at: http://technet.microsoft.com/en-us/sysinternals/default.aspx Accessed: 10 June, 2009

Emisisoft. (2009). Available at : http://www.emsisoft.com *Accessed: 10 June, 2009.*

Harley, D. and Lee, A. (2007) 'Testing, Testing: Anti-Malware Evaluation for the Enterprise', *10th Annual AVAR International Conference, Seoul 2007.* Available at: http://www.eset.com/download/whitepapers/TestingTesting(May2008).pdf Accessed: 10 January, 2009.

Harriman, J. (2006) 'A Testing Methodology for Antispyware Product's Removal Effectiveness'. *15th Annual EICAR Conference, 2006.* Available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/testing_methodology_for_antispyware_removal.pdf Accessed: 26 July, 2009

Hijackthis (2009). Availabe at: http://us.trendmicro.com/us/home/home-user/ Accessed: 11 June, 2009

Install Watch (2009). Available at: http://www.epsilonsquared.com/installwatch.htm Accessed: 11 June, 2009

Malware domain list.(2009). Available at: http://www.malwaredomainlist.com Accessed: 10 June, 2009

Marx, A. and Morgenstern, M (2008). *System Cleaning: Getting Rid of Malware from Infected PCs.* Available at: http://wwww.virusbtn.com/virusbulletin/archive/2008/06/vb200806-system-cleaning (Accessed: 10 January, 2009) Registration required.

Microsoft Baseline Security Analyser (2009). Available at: http://www.microsoft.com Accessed: 10 June, 2009

Microsoft (2008) *List of Anti-virus Software Vendors.* Available at: http://support.microsoft.com/kb/49500 Accessed: 10 July, 2009

Pandalabs (2009) *Annual Report Pandalabs 2008.* Available at:

http://pandalabs.pandasecurity.com/blogs/images/pandalabs/2008/12/31/annual_report_pandalabs_2008_ENG.pdf (Accessed: 23 June, 2009)

Process Explorer (2009). Available at: http://technet.microsoft.com/enus/sysinternals/default.aspx Accessed: 10 June, 2009.

Process Monitor (2009). Available at: http://technet.microsoft.com/en-us/sysinternals/default.aspx Accessed: 10 June, 2009.

Pstools (2009). Available at: Available at: http://technet.microsoft.com/en-us/sysinternals/default.aspx Accessed: 10 June, 2009.

Secunia Personal Software Inspector (PSI). Available at: http://secunia.com/vulnerability_scanning/personal/ Accessed: 15 July, 2009

R-Drive Image (2009). Available at: http://www.drive-image.com/ Accessed: 11 June, 2009

Regshot (2009). Available at: http://sourceforge.net/projects/regshot/ Accessed: 10 June, 2009

Regsnap (2009). Available at: http://lastbit.com/regsnap/ Accessed: 10 June, 2009

Rootkit Revealer (2009). Available at: http://technet.microsoft.com/en-us/sysinternals/default.aspx Accessed: 10 June, 2009.

Virustotal (2009). Available at: http://www.virustotal.com. Accessed: 15 July, 2009