2.7.1

Microsoft Antispyware

Version 1

Laboratory Overview

Objective

At the end of this lab students will be able to use Microsoft Antispyware to test a host for adware and spyware.

Information for Laboratory

A. Students will install Microsoft Antispyware
B. Students will test and remove adware/spyware
C. Students will use the System Explorer to study vulnerabilities

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Estimated Completion Time

30 Minutes

Adware/ Spyware

Adware is any software that displays advertisements through banners and popups. It's the software version of junk mail. Spyware is software that uses the Internet connection of a host in the background, and without the user's knowledge or consent, to track and send personal information to various parties. Obviously, Spyware is much worse since it involves an invasion of privacy.

Host computers acquire adware/ spyware by visiting certain web sites, and by downloading and installing certain software. Some shareware programs now inform you that the subject software is bundled with advertising software, and since the installation asks for your consent, technically this is not adware. The resulting nuisance is the same.

It has been estimated that over 80% of computers connected to the internet have adware/ spyware. As a host becomes infested with more and more of it, serious performance degradation will result.

Microsoft Antispyware

As a result of the prolific presence of adware/ spyware, several programs have been developed to mitigate the problem. Ad-aware, Spybot, and Pest Patrol are just a few of the programs available that provide free versions with more functionality upon purchase.

Recently, Microsoft Corporation has entered the fray. In December 2004, Microsoft purchased Giant Company Software. It's product, Giant Antispyware, has been modified and released January 2005 as Microsoft Antispyware Beta1.

Clearly, Microsoft is serious about addressing what has become a serious menace to Internet users.

Step I:
Execute the Microsoft Antispyware installation program on your lab PC, or located on a file share. Otherwise the install file can be downloaded from,

http://www.microsoft.com/athome/security/spyware/software/default.mspx

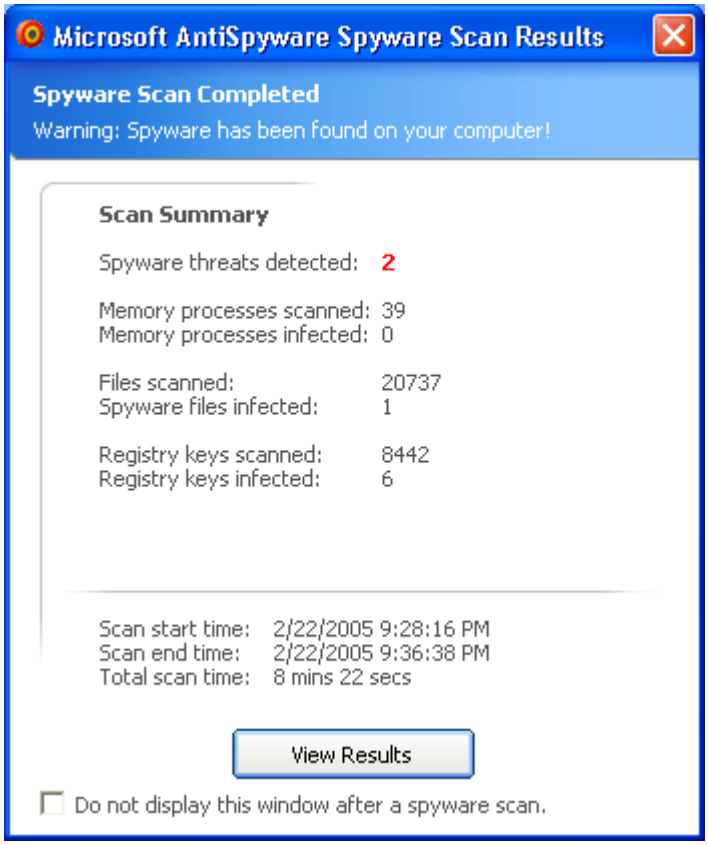
Follow the default parameters to complete the installation.

Step 2:
Update the spyware definitions,

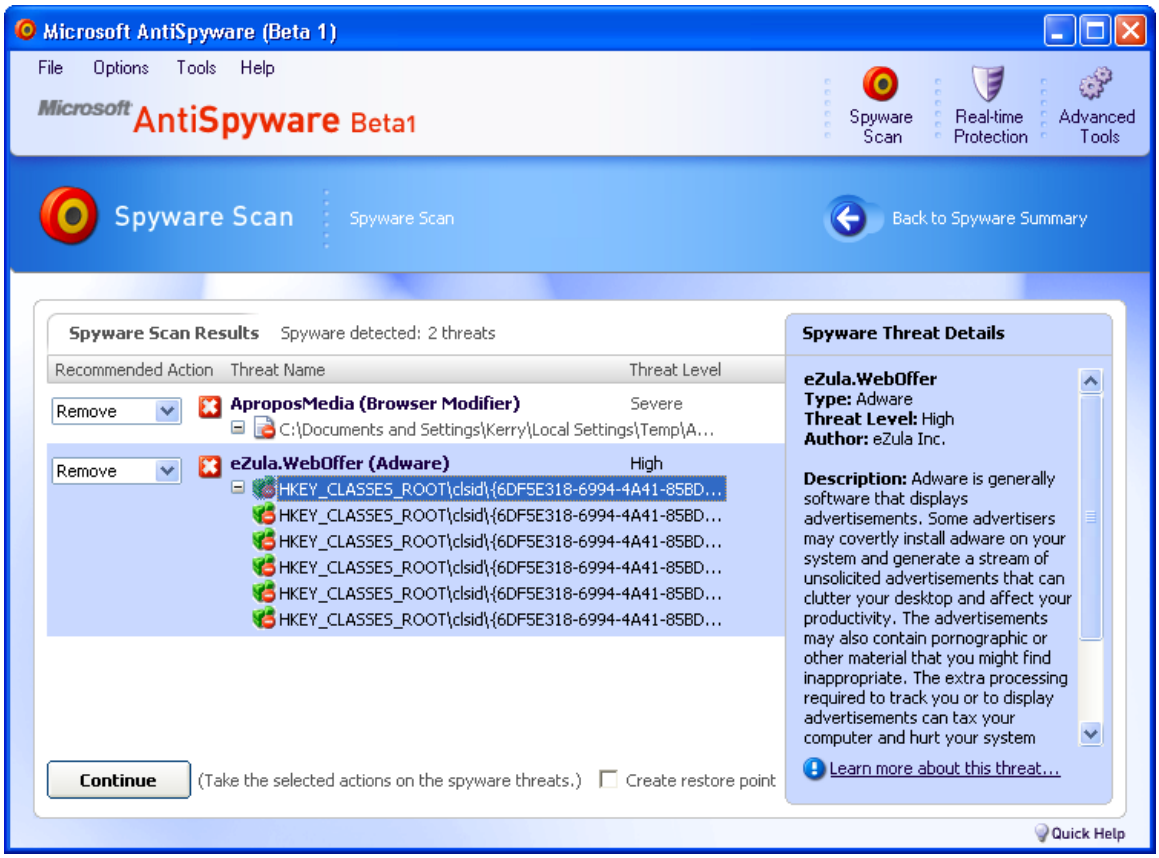
Note that Microsoft Antispyware might update definitions automatically. You may also use the drop down menu File-Check…
Step 3:

Start Microsoft Antispyware from the Start menu, and Run Quick Scan Now.

Microsoft Antispyware will scan memory, select files, registry keys, and cookies. Results of the scan will vary greatly depending on level of infection and integrity of definitions at the time of the scan.



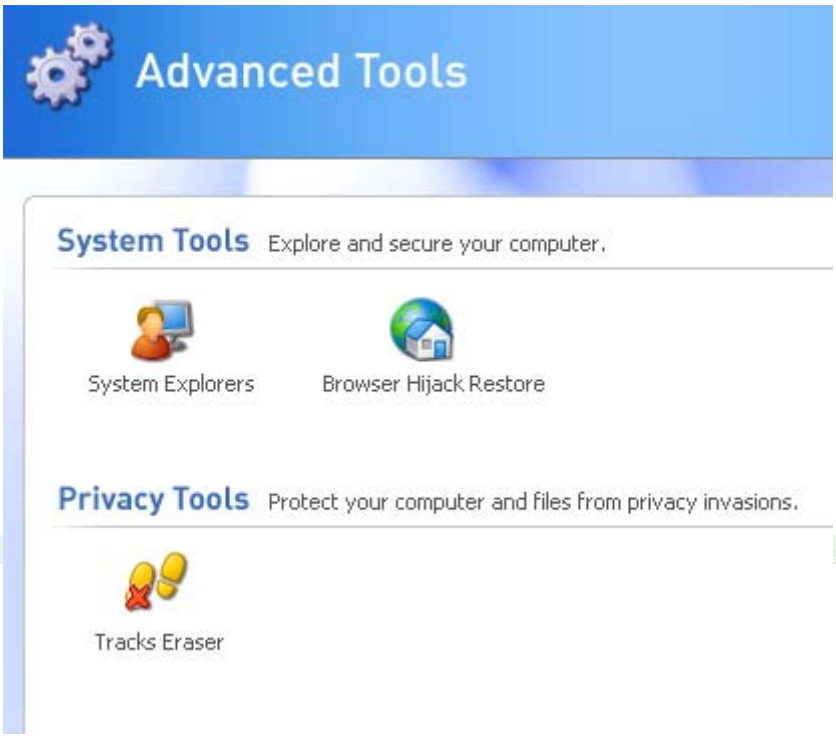
View the results and study the Spyware Threat Details.



Continue and remove the threats. Note that you can create a restore point prior to spyware removal.

Step 4
Explore Real-time Protection features. Microsoft Antispyware has the capability to stop adware/ spyware infection through its numerous security agents. Much can be learned about computer vulnerabilities by studying the details of real-time protections.

Step 5
Try using the advanced tools.



System Explorers offers the user a rich view of application, Internet Explorer settings and add-on programs, as well as networking and system information. Each System Explorer includes details of each entry together with an assessment of hazard level. Questionable, unknown hazards can be studies via an Internet search.

The Browser Hijack Restore tool mitigates alterations in Internet Explorer caused by various adware/ spyware. The use of an alternate browser such as Mozilla Firefox can sidestep adware/ spyware specifically designed for Internet Explorer.

The Tracks Eraser is designed to remove several application histories that may be the target of spyware. Auto completion of passwords, for example, always represents a vulnerability.

Analysis

1) Why did Microsoft Corporation purchase Giant Software Company and release Microsoft Antispyware?

2) Contrast the threat and impact of adware versus spyware.
3) Discuss ethical issues surrounding the use of adware/ spyware

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Search the Internet for studies and tests that have compared performance of various antispyware programs.

Appendix

This lab was performed using Microsoft AntiSpyware Version: 1.0.501.

The host operating system was Microsoft Windows XP Professional SP2.