DECLARATION OF ERIC B. COLE, Ph.D.

Eric B. Cole, declares and states as follows:

1. I am an independent computer security consultant and Dean of Faculty and Lead Instructor at the SANS (SysAdmin Audit Network Security) Institute, an information security training, certification, and research organization. I have served as the Director of Research and Chief Scientist at Sytex, Inc. and the Chief Security Officer at GraceIC. I also have served as an adjunct professor at Georgetown University and the New York Institute of Technology. I received my masters and B.S. degrees in Computer Science from the New York Institute of Technology, where I graduated *magna cum laude*, and received my Ph.D degree in Network Security from Pace University. My consulting, teaching, and research in part focus on computer security, intrusion detection, and malicious code, including spyware. My curriculum vitae is attached as Exhibit 1.

2. I received six exceptional performance rewards for my work as Internet Program Manager and Computer Engineer with the Office of Security at the Central Intelligence Agency. I have authored several articles and books, including *Hackers Beware* (2001) and a SysAdmin magazine article *Are Your Systems Really Safe* (2003). I am a member of the editorial board for Common Vulnerability and Exposures (CVE), which is federally-funded research project to develop standards for identifying, categorizing, and naming publicly known computer vulnerabilities and security exposures. I also serve on the editorial board for the HoneyNet Project, which is a project to evaluate hacker strategies and behavior. I am a member of the International Who’s Who in Information Technology and author and speaker for SANS Institute, and have frequently performed

consulting on Microsoft Systems. I am a Certified Information Systems Security Professional (CISSP).

3. For the purposes of this declaration, I use the term “spyware” to refer to software that gathers information about a computer’s use and transmits that information to a third party, without the computer user’s knowledge or consent. Spyware also may refer to software that appropriates resources of the computer that it infects, or alter the functions of existing applications on the affected computer. Adware refers generally to software that distributes online advertising to computers through the use of pop-up ads and other mechanisms.

4. Because of my expertise in computer science and distributed networks, the FTC requested that I evaluate the efficacy of the software program Kazanon 1.0 (“Kazanon”), which I downloaded from the web site www.kazanon.com. Specifically, the FTC requested that I evaluate whether there is evidence to support the claim that Kazanon makes users of file-to-file (“P2P”) sharing programs anonymous and therefore prevents any one from discovering their computers’ IP address, location, or their identity when they download or trade music, movies, software, or any other data, sound, or video files through the Internet.   The FTC also requested that I document and evaluate the effects of installing Kazanon on a computer. Finally, the FTC requested that I evaluate and document the process of removing Kazanon, including all components that are installed in conjunction with it, from the computer.

5. To form my conclusions, I observed the effects of downloading Kazanon from the web site www.kazanon.com onto a computer using a clean installation of the Microsoft Windows XP Operating System (“Windows XP OS”). Separately, I used P2P software to

initiate multiple file transfers from this computer to a different computer. I also used P2P software to initiate file transfers from a clean machine that did not have Kazanon installed. To gather data and analyze my test results, I used various forensic software tools and relied on my extensive experience in developing and deciphering software, in studying Internet-based distribution of spyware and other programs, in encrypting and decrypting code, and in securing and protecting computer systems.   To form my conclusions, I also referenced publicly available materials concerning the Windows OS and certain spyware and other programs, including *Microsoft Windows Internals*, *Windows Systems Programming*, and *Programming the Microsoft Windows Driver Model*.

SUMMARY OF FINDINGS

6. I found that Kazanon made no change in the behavior of the file transfers that I conducted using P2P software. Kazanon did not conceal the computer's IP address, location, or identity. I found that installing Kazanon to the computer causes numerous spyware, adware and other programs, including a program known as "Clientman," to be installed. When I refer to Clientman, I mean a group of files, including, but not limited to, msmc.exe and download-manager.exe, that cause the computer to, among other things, connect to the web servers omi-update.net and datastorm.biz. The FTC staff has informed me that these web servers are registered to Odysseus Marketing, Inc.   I found that Clientman and these other programs deposit numerous files, including executable files, on the computer and modify important existing files, including critical Windows OS files, which I discuss more generally in Paragraphs 29 and 30.

7. After installing Kazanon, I observed that the computer's web browser began to function differently. Among other things, when I conducted Internet searches using search engines such as Google and Yahoo, the results that the web browser produced differed in content from the results that the web browser produced on a computer without Kazanon installed. I also found that without a prompt from the user the computer's web browser automatically connected to various web servers, including omi-update.net, datastorm.biz, abetterinternet.com, speedera.net, flingstone.com, and skoobidoo.com. During these Internet connections, I observed that many packets containing data were being transferred from and to the computer. In addition, I found that a number of adware and other programs were installed to the computer without notice to the user. Finally, I found that when I opened the computer's web browser a number of Internet pop-up advertisements were displayed to the computer.

8. As discussed more generally in Paragraphs 27 through 29, 34 and 35, I found that after installing Kazanon, I could not easily locate and remove it and the other programs that it installed, including Clientman, from the computer. Kazanon and Clientman do not adhere to the standard procedures that are used to install software. The programs fail to create a folder in the Windows XP OS to store their files. The programs also do not create an icon on the desktop or in the Windows XP OS Start Menu. Because they do not create such a folder or icon, Kazanon and Clientman are not visible to the user. I also found that I could not remove Kazanon and Clientman using the standard "Add Remove" utility of the Windows OS. Further, Kazanon and Clientman do not provide their own uninstall tools. Finally, I found that the uninstall utility published at the web page www.oddysseusmarketing.com/uninstall did not fully remove Kazanon or Clientman, and

did not remove any of the additional programs installed by Kazanon. I found that the most efficient means to remove Kazanon and Clientman from the computer was to reinstall the entire OS.

SUMMARY OF CONCLUSIONS

9. My original analysis was conducted on November 15th, 2004, and a follow-up analysis on February 16, 2005. My analysis and conclusions are based on observations that I made and not on a study of Kazanon's source code. Specific details in this declaration, such as web server IP addresses, the web servers to which the web browser is instructed to connect, and the specific adware and other programs that are installed after downloading Kazanon, are based on the results and data that I collected on those specific days. As of the time this declaration was authored (September 7, 2005), some of these specific details may have changed, such as the specific web servers to which the web browser is instructed to visit and the content of these web servers, and have been (and continue to be) updated over time. However, my overall conclusions are still true: Kazanon fails to conceal the source of file transfers that are conducted using P2P software; Kazanon causes numerous spyware, adware, and other programs to be installed to the computer, and downloading Kazanon causes the computer's web browser to override search engine results and to automatically connect to various web servers without a prompt from the user.

10. Based on my research and professional expertise, I conclude that Kazanon does not make users of P2P programs anonymous and therefore does not prevent others from discovering their computers' IP address, location, or their identity when they download or trade music, movies, software, or any other data, sound, or video file through the Internet.

In my professional opinion, the main function, if not the only function, of Kazanon is to load spyware, adware, and other software onto the computer without the computer user's knowledge or authorization. In addition, based on my research and observations, as a result, installing Kazanon degrades the user's interaction with the Internet, including, but not limited to, replacing information that he or she receives from search engines such as Yahoo and Google. Further, in my opinion, the size and type of data that I observed being transferred from the computer to outside web servers during controlled tests are consistent with the transfer of personal information ("PI") from the computer.

11. In addition, in my professional experience, installing software in the manner used by Kazanon and Clientman is intended to make it difficult for users to detect the programs on the computer. However, to restore the computer to its original state prior to installation, in my professional opinion, Kazanon and the spyware, adware, and other software that is downloaded in conjunction with it, including Clientman, must be removed from the computer. Finally, based on my research and professional expertise, the average computer user would lack sufficient knowledge and experience to remove (uninstall) Kazaon and the spyware, adware, and other software that is downloaded in conjunction with it, including Clientman, without expending substantial time or resources.

BACKGROUND

12. Desktop and laptop personal computers ("PCs") are pre-loaded with operating system software ("OS"). The OS controls how the computer behaves and allows users to interact with the computer. Without the aid of the OS, the computer can not operate. The OS organizes and controls the computer's hardware and software resources, which

include the processor, memory, disk space, and any devices. As part of its resource management, the OS ensures that each computer process and application has sufficient memory and processor time to execute properly. An important feature of the OS is providing a set of protocols (commonly referred to as "hooks"), which are used by software applications running on the computer to perform constant computing functions, such as installing files or creating folders. These hooks allow software developers to create programs that do not have to address changing details of computer hardware, and can rely on the OS to handle it for them.

13. Most PCs are pre-loaded with the Microsoft Windows Operating System ("Windows OS"). The current version of the Windows OS is "Windows XP." The Windows XP OS typically is pre-loaded in the primary partition of the computer's hard disk. By default, a folder named "Windows," which is mapped to C:\WINDOWS, is created to store the Windows XP OS software. There are dozens of subfolders located in the Windows folder, including "System32," "Prefetch," "Temp," and "Last Good." The subfolder "System32" in the Windows folder contains more than 400 files, including *all the files that enable core OS functions*. These core files are responsible for functions such as saving programs to the hard-drive. Among the core files that are stored in the System32 folder are "mycomput.dll," Win32k.sys," "Kernel32.dll," "Advapi32.dll," "User32.dll," and "Gdi32.dll."

14. Other Windows subfolders that are created during a default installation of the Windows XP OS tend to contain a smaller number of files and are associated with targeted functions. For example, the "Prefetch" folder contains frequently used portions of files and applications, which the OS automatically loads during the start-up process to

conserve time. Another subfolder, the "Temp" folder, as its name indicates, stores temporary OS and application files. A third folder called the "Last Good" preserves a copy of the computer's configuration at the time it boots. In the event the computer crashes or otherwise malfunctions, the OS relies on this configuration in the "Last Good" folder to restore the computer.

15. The OS also serves a crucial role in facilitating the installation and removal of software applications. The Windows XP OS (as well as other versions of the Windows OS) include technology known as the "Windows Installer," which manages the installation of applications; diagnoses and repairs corrupted files; and prevents conflicts with other applications. During a standard Windows installation, the OS's Windows Installer detects when a program is installed, records all changes that it makes to the computer, and creates an entry in the OS's "Add/Remove" utility. This utility is located in the Control Panel as part of the Start Menu. The Add/Remove utility is designed to list the programs that are installed on the computer and enable users to remove any program with ease. Microsoft publishes specific guidance for programmers on how to enable the Windows Installer, which involves including four lines of additional code in the program. *See, e.g.* Brian Noyes, *Deploy Apps With Ease* (last modified Jan. 25, 2004), at http://searchvb.techtarget.com/vsnetTip/1,293823,sid8_gci945897_tax293033,00.html. A copy of the Microsoft-sponsored guide is attached as Exhibit 2.

16. In writing a program, the programmer builds the core program, specifies where the program's files are to be stored on the computer's hard drive, and finally, develops an uninstall tool that can remove the program. During installation, it is standard practice to create a single folder in which to store the program's files. This folder is placed in the

Windows XP OS's "Program Files" folder and typically is given a name that conveys its association with the program. More complicated programs may deposit a few files in other OS folders, usually the System32 folder. These files are deposited in the System32 folder because they enable functions that could be shared by multiple programs. For example, different word-processing programs may use the same file to perform a shared function such as selecting font size. Although in some cases a sophisticated program may deposit a few files in the System32 folder, it is not considered an acceptable practice for programs to modify or override files in that folder, especially any core OS files.

17. As part of a standard installation, a program directs the Windows XP OS to create an icon, either on the desktop or in the Start Menu, which represents the program to the user. This icon links to the program's folder located in the OS's Program Files folder. Like most OSs, the Windows XP OS uses a Graphical User Interface ("GUI") to interact with the user. A GUI publishes icons, symbols, and images, rather than just text. Thus, a program's creation of an icon using the GUI makes the program visible to the user after it is installed.

18. In providing an uninstall tool, the programmer can either (1) rely on the default Add/Remove utility that the OS provides; or (2) create a specific uninstall tool for the program. By default, unless a program is written to avoid detection by the Windows XP OS, a program will be published in the OS's Add/Remove utility. If a user selects to remove a listed program, the utility automatically reverses any changes it made to the computer.   The programmer also could develop an uninstall tool for the program and include it. In the computer field, it is considered better practice for programs to have their own uninstall tools. Typically programmers use widely-available wizard programs

to develop uninstall tools. These wizard programs display a series of screens to the user during the program's installation and removal. The user can go directly to the program, either on the desktop or in the Start Menu, and activate the uninstall process. Even if a program has its own uninstall tool, it continues to appear in the Windows XP OS's Add/Remove utility. In cases where the user activates removal through the Add/Remove utility, the utility is directed to use the program's own uninstall tool to remove the program.

METHODOLOGY

19. To conduct my research and form my opinion, I used multiple clean computers with Windows XP OS and the Microsoft Internet Explorer web browser ("IE web browser") installed. Using some of the computers, I visited the web site www.kazanon.com and clicked on the link "Kazanon 1.0 Download" to download Kazanon. One computer remained at baseline; Kazanon was not installed on this computer. I conducted a series of tests using these computers to determine: (a) Kazanon's effectiveness in concealing the IP address, location, or identity of computers sharing files with P2P programs; (b) the effects on computers of installing Kazanon, including any data transfers from the computer to third parties; and (c) the process of installing and uninstalling Kazanon.

20. To test Kazanon's efficacy, I conducted data transfers on computers with Kazanon installed. I used two different P2P programs – Kazaa and Morpheus -- to conduct these data transfers and analyzed the data that a second computer received. I also compared the results to data transfers that I conducted on computers that did *not* have Kazanon installed.

21. To evaluate the effects on the computers that had Kazanon installed, I visually observed the effects on the computer; recorded and analyzed data flowing in and out of the computer; and tracked changes made to the computer system. During the first 30-minute period immediately after installing Kazanon, I kept the computer idle. I recorded all network traffic flowing in and out of the idle computer during this 30-minute period. Finally, I used software programs that monitor changes to the computer's registry and files and detect whether files or programs have been created, modified, or deleted.

22. I also performed directed tasks on separate computers. Specifically, using a computer that had Kazanon installed and a computer that did *not* have Kazanon installed, I conducted searches on a number of search engine web sites, including www.google.com and www.yahoo.com, and compared the results that these web sites produced. Separately, in an effort to determine whether downloading Kazanon caused personal information to be collected, I attempted to decrypt data packets flowing out of the computer. Using both a computer that had Kazanon installed and a computer that did not, on multiple occasions I entered information into a banking web site and recorded network activity after entering this information. I then compared the data flowing out of the computer that had Kazanon installed with the data flowing out of the computer that did not have Kazanon installed.

23. In addition, to evaluate how Kazanon is installed and uninstalled, I visually observed the computer when I downloaded the software and when I attempted to uninstall it. I also monitored registry and file changes that were made to the computer system. To uninstall Kazanon, I attempted to locate it first in the "Add/Remove" utility of the Windows XP OS, and second, on the desktop of the computer. I then followed the

instructions that were published at www.odysseusmarketing.com/uninstall to uninstall Kazanon.

ANALYSIS AND RESULTS

Testing of Kazanon

24. To test Kazanon's efficacy, I used a two-phase approach. First, I loaded two different P2P programs -- Kazaa and Morpheus -- onto two separate computers that had Kazanon installed. I used these P2P programs to send packets of data to a second computer. I then observed the data that the second computer received. I found that when I conducted data transfers with both Kazaa and Morpheus the IP address and location of the sending computer was available to the receiving computer, and therefore the data's source was not concealed.

25. For the second test, I loaded the P2P programs Kazaa and Morpheus onto two computers that did *not* have Kazanon installed. I sent data to a second computer using these computers. I then made the same data transfers using computers that had Kazanon installed. I compared the type and size of the data, including network protocol header, sent to the second computer from computers that had Kazanon installed and from those that did not. The network protocol header contains information that is used to determine where and how data is sent between computers.

26. In cases where software acts to conceal the source of a data transfer, the data sent out of a computer is altered in size and type and the network protocol header is not revealed. I found, however, that the data packets originating from computers that had Kazanon installed did not differ in size and type from data packets originating from computers that did *not* have Kazanon installed. I also found that the network protocol

information was not concealed. Therefore, based on the controlled tests that I performed, I conclude that Kazanon does not conceal the IP address, location, or identity of computers sharing files with P2P programs. Further, in my professional opinion, the sole purpose of Kazanon is to download additional software, including spyware, to computers.

Effects on Computers After Kazanon Is Downloaded

27. After I initiated a download of Kazanon, I observed that the file "download-manager.exe" had been installed onto the computer at C:\down\download-manager-exe. I also observed that the file "msmc.exe" had been installed in the OS's System32 folder, which, as explained in Paragraph 13, contains critical OS files. Further, the msmc.exe file caused numerous additional files, components, and registry keys to be downloaded to the computer. Msmc.exe and many of these files contained a data stamp that preceded the date on which Kazanon was installed.[1] Also, this msmc.exe file and many of the additional files that it downloaded make-up the program that I refer to as Clientman.

28. Once the Kazanon download began, there was no opportunity to stop it or the installation of Clientman. Further, I did not receive any prompts indicating that the Kazanon or Clientman downloads had even occurred. In fact, I found no icon representing Kazanon or Clientman on the desktop or in the OS's Start Menu after installation. I also found no new folder for Kazanon or Clientman in the Windows XP OS's Program folder. Thus, in my opinion, given the stealth techniques employed to install Kazanon and Clientman, the average consumer would not detect the presence of these programs on their computers.

[1] I also evaluated software products distributed through the web sites www.sweepstakes-hq.com, www.essential-free-downloads.com, and www.downloads-for-free.com. The FTC staff has informed me that these web sites are registered to Odysseus Marketing, Inc. I found that the software products that these web sites distribute downloaded the same or substantially similar files, components, and registry keys that Kazanon downloaded.

29. I continued to observe the computer during a 30-minute period after I downloaded Kazanon. During this time, there were hundreds of instances where files had been created, modified, or deleted on the computer. For example, I observed that new files had been added to the OS folders System 32, Prefetch, and Last Good. As discussed in Paragraph 14, adding new files to these folders affects the programs that the computer automatically loads during start-up and the system configuration the computer uses to restore itself in the event of a crash. I also detected that critical files in the OS's System 32 folder had been corrupted, including the files "mycomput.dll," Win32k.sys," "Kernel32.dll," "Advapi32.dll," "User32.dll," and "Gdi32.dll." It is well accepted in my field that under no circumstances should software modify critical OS files stored in the System32 folder.

30. Immediately after Kazanon was downloaded, I found, among others, the following programs had been installed: Clientman, VX2, Avenue A, Blazefind, Ncase, InternetOptimizer, BargainBuddy, WebRebates, eZula, FastClick, Sexlist, and DSO Exploit. A couple days after downloading Kazanon, I discovered the following programs: Advertising.com, Bfast, ClickAgents, HitBox, HitLink, Ie Plugin, TargetNet and WebTrends Live. These programs were downloaded automatically without any prompt. I also found, among others, the following new processes running on the computer after Kazanon was installed: msmc.exe, wsup.exe, wtoola.exe, wtoolS.exe, and PIB.exe.

31. During the 30-minute period after I downloaded Kazanon, I observed that the computer automatically connected to a number of different web servers. Immediately after the download, the computer connected to the IP addresses 216.22.28.235 and

216.22.28.231, which the FTC staff has informed me are associated with the domain names omi-update.net and datastorm.biz. I further discovered that during this period the computer connected to several other IP addresses from which it downloaded information. A chart listing some of these IP addresses and the domain names with which they are associated is attached as Exhibit 3.

32. In monitoring network activity, I detected that the web servers omi-update.net and datastorm.biz downloaded information to the Kazanon-installed computer and uploaded information from it. On a regular basis, I found that outbound transfers occurred at a minimum 1 to 2 times per 18 hour period. The information that datastorm.biz uploaded was encrypted and therefore unreadable by unauthorized parties. Because the web server used a high-level of encryption, decoding it would require me to expend substantial time and resources. Instead, I performed a dozen controlled tests on a banking web site using both a computer that did and did not have Kazanon installed. On this web site, I entered banking information into online forms and monitored the computer's outbound activity. Each time I entered the information using the Kazanon-installed computer, I detected outbound data transfers of a similar size and type to the web server datastorm.biz. I also compared this network activity to that of the computer that did not have Kazanon installed. In my opinion, the network activity that I detected on the Kazanon-installed computer is consistent with the transfer of the entered banking information from the computer.

33. Upon launching the IE web browser on a computer that had Kazanon installed, a number of pop-up ads appeared, including ads promoting "Tickle" IQ and Personality Tests, SpywareNuker anti-spyware, "Bullseye Network" offers, a MyDietPatch product,

and a free laptop computer. I also conducted directed Internet searches using the search engine web sites www.google.com, www.yahoo.com, and www.lycos.com. I found that the search results that these search engine web sites would normally produce were modified. For example, in conducting an Internet search for the term "Adaware," I found that in the case of each of these web sites the search results that were displayed to a computer that had Kazanon installed differed substantially from those that were displayed to a computer that did *not* have Kazanon installed. Screen shots of the displayed search results are attached as Exhibits 4 and 5.

Uninstalling Kazanon and Clientman

34. In attempting to uninstall Kazanon, I found that neither Kazanon nor the program that it installs – Clientman – appeared in the OS's Add/Remove utility. Therefore, I could not use the OS's default uninstall utility to remove the programs. I also could not locate the programs on the desktop or in the Start Menu. Thus, to uninstall Kazanon or Clientman manually, I would have to locate each file, registry key, and other component that the programs had installed and remove each file, registry key, and other component separately.

35. Second, I attempted to uninstall Kazanon and Clientman using the uninstall utility published at www.odysseusmarketing.com/uninstall, which the FTC staff had provided to me. A copy of this web page is attached as Exhibit 6. After following the instructions published on the web page, I found that the programs had not been uninstalled. Specifically, I analyzed changes to computer registry and hard drive and found that many files installed by Kazanon and Clientman, including msmc.exe, had not been removed from the computer. I also found that new files had been added to the computer after the

purported uninstall. I further observed that the effects I reported in Paragraphs 29 through 32 continued to occur on the computer.

CONCLUSIONS

Based on the forensic testing that I conducted, and my training, expertise, and research experience in computer security and spyware, I conclude that:

(a) Kazanon does not make users of P2P programs anonymous and therefore does not prevent others from discovering their computers' IP address, location, or their identity when they download or trade music, movies, software, or any other data, sound, or video file through the Internet;

(b) Kazanon's main function, if not its only function, is to load spyware, adware, and other software onto the computer without the computer user's knowledge or authorization;

(c) Kazanon and Clientman degrade the user's interaction with the Internet, including, but not limited to, replacing information that he or she receives from search engines such as Yahoo and Google;

(d) The network activity that I observed after Kazanon and Clientman had been downloaded is consistent with PI being collected from the computer;

(e) Kazanon and Clientman do not adhere to the standard procedures that are used to install software;

(f) The average computer user would lack sufficient knowledge and experience to remove (uninstall) Kazaon and the spyware, adware, and other software that is downloaded in conjunction with it, including Clientman, without expending substantial time or resources.

Dated: September 10, 2005 /s/ Eric B. Cole

Eric B. Cole, Ph.D.