

**[0015]** Several techniques exist that are effective for detecting some forms of malicious code. For example, some types of malicious code can be detected by examining the binary code image of the program during its execution or the binary code image of the program when it is stored on a storage device. Many malicious code programs can be identified by a unique bit or byte pattern. The unique bit or byte pattern can include the entire image of the program while it is stored in memory or while it is stored on disk. The signature can also be a bit or byte pattern that is a portion of the program in memory or on disk. Once the unique sequence has been identified, a signature can be developed to identify the sequence. The signature is often the bit or byte pattern itself or it is in the form of a checksum. A detection program can then search for a malicious code program using the signature to identify the unique bit or byte sequence. Trojans, however, may be configurable to have no easily identifiable signature. Trojans may have configuration parameters that change the bit or byte sequences in the program and make it difficult or impossible to provide a unique signature. Various tools can be used to reconfigure a trojan, so that it will not have a known signature.

**[0016]** Another technique used to identify trojans examines the behavior of a trojan server while the trojan server is loaded and installed on a computer. With such a technique, a loaded and installed program is first placed into a sandbox, which includes a restricted area on the computer where the program (e.g., trojan server) can be examined safely. While such an approach may be effective for preventing some trojan infection, the approach does not however detect trojan servers once they are already installed on a computer. Such an approach does not detect many trojan servers because trojans do not exhibit their most characteristic behaviors while they are being loaded or installed, but rather they come alive and exhibit their malicious behavior after they have been loaded and installed.

**[0017]** Remote control software ("remote control"), such as pcAnywhere and VNC, is another type of malicious code, which has much of the same functionality as trojans. These programs allow for remote administration (via a "client" on a host personal computer ("PC")) of a target PC that is executing the "server" portion of the program. A goal of a trojan is to be stealth and transparent to the innocent victim, so as to remotely control the PC or other machine. By comparison, a goal of remote controls is to allow a trusted remote user to administer the machine for efficiency purposes. Nevertheless, remote controls can also be used by an evil hacker to remotely control a machine that is "infected" by the unauthorized remote control, in a stealthy and malicious manner. Moreover, even if a remote control is operated by a trusted legitimate user, the remote control can also be used by malicious individuals if proper security precautions are not taken (e.g., password protection, authentication, encryption). Accordingly, remote controls can be used for malicious purposes, so the present disclosure relates to them as well.

**[0018]** Keystroke loggers ("keyloggers" or alternatively "keyboard loggers") are another type of malicious code. The keylogger is executable code that can exist in one of many forms. For example, some forms of keyloggers can be instantiated in executable code as one or more programs, computer files, threads inside other programs, plugins or shared modules loaded by other programs, or modules

loaded into operating system kernel memory in the manner of a device driver or loadable kernel module. A keylogger is a form of malicious code that enables a person to obtain the actual "punched" keystrokes from an infected computer. A record of the keystrokes usually exists in the form of a file on the file system, which stores the "punch for punch" results of what was typed at the keyboard. Also, some keyloggers provide capability for e-mailing (to an e-mail address) a record of the captured keystrokes, in order to share access and remotely identify the typed characters. Alternate access mediums are sometimes used for obtaining a record of the keystrokes, such as physical access to the infected system, e-mailing a file to a configured e-mail account, or "backdoor" access to the machine via a trojan. Sinred, Fearless KeySpy, and TeeJayEm KeySpy are examples of keyloggers. Typically, a keylogger is a software application (e.g., which may be, but is not necessarily, a standalone application) that exists in a machine's operating system.

**[0019]** Monitoring software is another type of malicious code, which has many similarities to keyloggers. In many respects, monitoring software performs operations that are similar to a keylogger. Monitoring software is often used to monitor a wide range of the computer's activity. For example, monitoring software is useful for a person to obtain a recorded log of actions that children, a spouse, friends, co-workers and others perform on their computers. Unlike keyloggers, monitoring software is often, but not always, purchased from a software vendor and installed by the computer's owner to achieve a new layer of surveillance over the computer owner's machine.

**[0020]** Spyware is an Internet term for advertising supported software ("adware"). Spyware differs from other malicious code, because spyware has legitimate purposes, in addition to potentially malicious purposes. Spyware is installed in a computer, according to a variety of techniques. Spyware's primary purpose is the gathering of marketing and statistical information about a user's electronic behavior, together with the reporting of such information via the infected machine's Internet connection to one or more collection servers via the Internet. According to the privacy policies of many advertising companies that develop and distribute spyware, no sensitive information (or other information that identifies the individual user) is authorized to be collected from the user's computer. Such a policy is helpful to allay possible concerns regarding invasion of privacy or malicious purpose. Nevertheless, such policies are not always adopted or followed. Many spyware examples contain a "live" server program executed by the machine, which is capable of sending personal information and web-surfing habits to a remote location. Accordingly, spyware is also covered by the present disclosure, because spyware can be used for malicious purposes.

**[0021]** Spyware has resulted in congestion of Internet web pages, as an increasingly large number of vendors create and distribute spyware via Internet sites that attract visitors. Spyware has also become a popular technique for shareware authors to profit from a product, other than by selling it directly to users. For example, if a user prefers, it can freely install an application bundled with spyware, instead of purchasing a license to the application. Several large media companies offer to place banner advertisements in software products, in exchange for a portion of revenue from sales