

resulting from the software products' display of the banner. This technique has increased in popularity, because users can avoid paying for the software products, and the software product developers receive money from alternate sources. If the user is annoyed by the banners, the user is usually given an option to remove them by paying a regular licensing fee for the software products.

[0022] Spyware is not illegal, but it raises various privacy issues for certain users. Such privacy issues are raised when the spyware tracks and sends information and statistics via a private Internet connection that operates in the "background" of the user's PC, using a server program that is installed on the user's PC. In a written privacy statement, legitimate adware companies will disclose the nature of such information that is collected and transmitted, but the user is typically unable to actually control it.

[0023] Worms are another type of malicious code that exists in a variety of different forms. For example, some (but not all) forms of worms are 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. Worms are distributed ("spread") via a computer network, such as the Internet. From the computer network, they penetrate a computer's memory, calculate network addresses of other computers, and send copies of themselves to such addresses for additional replication. Worms often exploit OS, application or service vulnerabilities to propagate themselves and penetrate remote machines. Worms have various purposes, designs, propagation media, and techniques for exploiting vulnerabilities. On the machine, worms may deposit a "payload," which performs some or no operation. Frequently, this payload includes a trojan or keylogger. Examples of worms are Code Red and Sircam. Worms are convenient vehicles for evil hackers to distribute other types of malicious code.

[0024] Viruses are another type of malicious code that can exist in a variety of different forms, such as macro viruses, boot sector viruses, and parasitic viruses. For example, some (but not all) forms of viruses are 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. Some viruses merely replicate by inserting (or attaching) themselves to a medium, in order to infect another program, boot sector, partition sector, or document that supports macros. But many viruses additionally inflict a large amount of damage on the machine. On the machine, viruses may deposit a payload, which performs some or no operation. Frequently, this payload includes a trojan or keylogger.

[0025] Malicious code, such as trojans, keyloggers, worms and viruses, can be used by evil hackers to disrupt the normal operation of the innocent victim's computer, to spy on the innocent victim, to steal money from the innocent victim, or to steal intellectual property from the innocent victim. The evil hacker often uses the innocent victim's computer to perform these malicious activities, in order to harm the innocent victim's associated organization (e.g., company or government). Accordingly, such malicious code

can harm a computer system, irrespective of whether the computer system belongs to an individual or an organization.

[0026] Information handling system **10** includes one or more of: a central processing unit (CPU) **12**, memory **14**, input/output (I/O) devices, such as a display, a keyboard, a mouse, and associated controllers, collectively designated by a reference numeral **16**, a hard disk drive **18**, or other storage devices or media drives, such as a floppy disk drive, a CD-ROM drive, a DVD drive, and memory device, collectively designated by a reference numeral **20**, and/or various other subsystems, such as a network interface card or wireless communication link (collectively designated by a reference numeral **22**), all interconnected, for example, via one or more buses (shown collectively as a bus **24**). Examples of information handling systems are a personal computer system, a personal digital assistant, a thin client device, a thick client device, or similar information handling device.

[0027] In one embodiment, the information handling system (IHS) **10** is configured with a suitable operating system for installing and executing instructions from one or more computer readable media **26**, such as a hard disk drive, floppy diskette, CD-ROM, DVD, or memory. Information handling system **10** may further be configured for communicating with another information handling system **28** (e.g., through a network **30** via a suitable communication link or links). The operating system of IHS **10** may optionally include instructions for installing and executing programs, and for downloading information via network **30**. The illustrative embodiments of the present disclosure may be practiced over an intranet, the Internet, virtual private network, or other suitable communication network.

[0028] According to one embodiment, the technique for malicious code detection is implemented in the form of computer software, the computer software including instructions executable by the CPU of a computer system, such as an innocent victim's computer system. The instructions include suitable program code processable by the computer system for performing the various functions as described herein. The various functions as discussed herein can be programmed using programming techniques well known in the art.

[0029] One technique for detecting malicious code includes a technique for detecting the portion of the malicious code that resides on a target computer system, such as an innocent victim computer system. For some forms of malicious code, such as keyloggers and Viruses, all of the malicious code resides on the innocent victim's computer system. For other forms of malicious code, such as trojans and remote controls, only the server portion of the malicious code resides on the innocent victim's computer system. The procedure can be embodied in a computer program, such as a malicious code detection program. The malicious code detection program detects the presence of (and identifies) the malicious code before, during and/or after the malicious code executes on the victim's computer system.

[0030] FIG. 2 illustrates an architecture of a malicious code detection program **40** that is executed by the information handling system **10** according to an embodiment of the present disclosure. The malicious code detection program **40** includes detection routines **42** and a scoring algorithm **44**.