

METHOD AND APPARATUS FOR DETECTING MALICIOUS CODE IN AN INFORMATION HANDLING SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to and is a continuation-in-part of co-owned co-pending U.S. patent application Ser. No. 10/231,557, filed Aug. 30, 2002, by Obrecht et al., entitled METHOD AND APPARATUS FOR DETECTING MALICIOUS CODE IN THE FORM OF A TROJAN HORSE IN AN INFORMATION HANDLING SYSTEM, which is incorporated herein by reference in its entirety.

BACKGROUND

[0002] The present disclosure relates generally to information handling systems, and more particularly to a method and apparatus for detecting malicious code in an information handling system.

[0003] Malicious code is computer software code that is executed by an information handling system, typically a computer (but it can also be a Personal Digital Assistant, embedded system, or other information handling device), and can be used for malicious purposes, such as damaging, altering or using the system without permission or knowledge of the system's owner or user, even if the code also has legitimate purposes. There are many different types of malicious code, such as trojan horses, remote control software, keystroke loggers, spyware, worms, viruses, and monitoring software.

[0004] Accordingly, a need has arisen for a method and apparatus for detecting malicious code in an information handling system, in which various shortcomings of previous techniques are overcome.

SUMMARY

[0005] Malicious code detection code is executed by an information handling system. The malicious code detection code includes detection routines. The detection routines are applied to executable code under investigation. The detection routines associate weights to respective code under investigation in response to detections of a valid program or malicious code as a function of the detection routines. It is determined whether code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines.

[0006] It is a technical advantage that various shortcomings of previous techniques are overcome.

BRIEF DESCRIPTION OF THE DRAWING

[0007] FIG. 1 is a system block diagram of an information handling system for detecting malicious code, according to one embodiment of the present disclosure; and

[0008] FIG. 2 is a process diagram of a detection architecture of a malicious code detection program, according to one embodiment of the present disclosure.

DETAILED DESCRIPTION

[0009] FIG. 1 is a system block diagram of an information handling system 10 (or "computer" or "computer system" or

"machine") for detecting malicious code, according to one embodiment of the present disclosure. Although the present disclosure describes some of the most common forms of malicious code, the present disclosure relates to all forms of malicious code.

[0010] Malicious code is computer software code that is executed by an information handling system and can be used for malicious purposes, such as damaging, altering or using the system without permission or knowledge of the system's owner or user, even if the code also has legitimate purposes. For example, a remote control program can be used by a system administrator to perform legitimate operations on another user's computer, but the remote control program may nevertheless be considered malicious code, because it can also be used for malicious purposes. Code is embodied in the form of one or more executable instructions and/or their associated operands for an information handling system ("programs" or "computer programs"), according to a variety of techniques, such as an independent program, a library, a thread, a routine or subroutine, or an operating system component, any of which can be written in any computer programming language (e.g., scripting languages, interpreted languages, compiled languages, assembly languages or machine code).

[0011] Malicious code is stored in any computer-readable medium, such as a hard disk drive, floppy diskette, CD-ROM, DVD or memory. During operation of an information handling system, malicious code has one or more states, such as active, inactive, executing (or "running"), not executing, hidden or visible. In the illustrative embodiments, the malicious code detection program is operable to detect malicious code, irrespective of the malicious code's states, and irrespective of the computer-readable media storing the malicious code.

[0012] Trojan horses ("trojans") are a particular type of malicious code. The trojan is executable code that exists in a variety of different forms. For example, some (but not all) forms of trojans are instantiated in executable code as one or more programs, 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 trojan is a form of malicious code that enables a person to remotely control someone else's computer. The person who remotely controls the computer is known as the "Evil Hacker" (or "hacker") while the person whose computer is being remotely controlled is known as the "Innocent Victim" (or "victim"). BackOrifice2000, SubSeven, NetBus and Optix-Pro are all examples of trojans. Trojans are sometimes referred to as "back-doors" or "hacker back-doors."

[0013] Most trojans have two components, the client program (trojan client) that is executed by the evil hacker's computer and the server program (trojan server) that is executed by the innocent victim's computer. Some trojans have only a trojan server that can be remotely controlled through manually entered commands rather than through the programmatic interface of a trojan client.

[0014] There are many ways to infect a computer with a trojan including sending the innocent victim the trojan server disguised as a valid program, copying the trojan server onto the innocent victim's computer, or exploiting a vulnerability in the innocent victim's computer to place the trojan server on the computer.