

on the computer system. Execution of the computer program continues until all active programs on the computer system have been tested and evaluated. Alternatively, other criteria may be established for a duration of testing with the malicious code detection program. For example, execution of the malicious code detection program can be configured to occur in response to one or more of a random initiation and a periodic initiation.

[0055] According to another embodiment, the malicious code detection program includes a small program configured for being delivered quickly, as well as, for being executed quickly. The malicious code detection program can be delivered to the innocent victim's computer over a network, such as a Local Area Network (LAN), Wide Area Network (WAN), Internet, intranet, or any other global computer network 30. The malicious code detection program may also be delivered via suitable computer readable media, such as, media 26 shown in FIG. 1.

[0056] While not stopping an infection of the computer system with malicious code programs, the technique of the present embodiments identifies a malicious code program when executing on a computer system. The technique for identifying a malicious code program is suitable for combination with other techniques, such as a technique for detecting infection, resulting in a more robust computer system malicious code protection implementation.

[0057] Where the foregoing disclosure mentions that code performs an operation, it is understood that the information handling system performs the operation in response to the information handling system's execution of the code.

[0058] Although illustrative embodiments have been shown and described, a wide range of modification, change and substitution is contemplated in the foregoing disclosure and, in some instances, some features of the embodiments may be employed without a corresponding use of other features. Accordingly, all such modifications are intended to be included within the scope of the embodiments. Accordingly, it is appropriate that the appended claims be construed broadly. In the claims, means-plus-function clauses are intended to cover the structures described herein as performing the recited function and not only structural equivalents, but also equivalent structures.

What is claimed is:

1. A method for detecting malicious code in an information handling system, comprising:

executing malicious code detection code (MCDC) on the information handling system, the MCDC including detection routines;

applying the detection routines to executable code under investigation, the detection routines associating weights to respective code under investigation in response to detections of a valid program or malicious code as a function of the detection routines; and

determining whether code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines.

2. The method of claim 1, wherein the detection routines include valid program detection routines and malicious code detection routines.

3. The method of claim 1, wherein the applying comprises:

applying the detection routines to gather information about the executable code under investigation by at least one of the following: examining the code or program; and searching for information in the information handling system about the code or program.

4. The method of claim 1, wherein determining whether the code under investigation is a valid program or malicious code includes scoring the execution of the detection routines as a function of the weights.

5. The method of claim 4, wherein scoring includes configuring a scoring algorithm to identify code under investigation as malicious code in response to at least one of a valid score and a malicious code score.

6. The method of claim 1, wherein the malicious code includes a trojan horse.

7. The method of claim 1, wherein the malicious code includes remote control software.

8. The method of claim 1, wherein the malicious code includes a keystroke logger.

9. The method of claim 1, wherein the malicious code includes spyware.

10. The method of claim 1, wherein the malicious code includes a worm.

11. The method of claim 1, wherein the malicious code includes a virus.

12. The method of claim 1, wherein the malicious code includes monitoring software.

13. A method for detecting malicious code in an information handling system, comprising:

executing malicious code detection code (MCDC) on the information handling system, the MCDC including detection routines for gathering information about executable code under investigation, the detection routines including at least one of the following: (a) examining the code or program and (b) searching for information in the information handling system about the code or program, the detection routines including valid program detection routines and malicious code detection routines;

applying the detection routines to the executable code under investigation, the detection routines associating weights to respective code under investigation in response to detections of a valid program or malicious code as a function of at least one of the detection routines; and

determining whether code under investigation is a valid program or malicious code as a function of the weights associated by the detection routines, wherein determining whether the code under investigation is a valid program or malicious code includes scoring an execution of the detection routines as a function of the weights, and wherein scoring includes configuring a scoring algorithm to identify code under investigation as malicious code in response to at least one of a valid score and a malicious code score.

14. The method of claim 13, wherein the malicious code includes a trojan horse.

15. The method of claim 13, wherein the malicious code includes remote control software.