

The detection routines **42** operatively couple to the operating system **46** of the computer system under investigation via application programming interfaces (APIs) **48**. The detection routines also access process behavior information (e.g., data) **50** and binary image information **60**, according to the particular requirements of a corresponding detection routine, further as discussed below.

[0031] In one embodiment, the malicious code detection program operates as follows. The malicious code detection program executes at any time, on an as-needed basis, a periodic basis, a random basis, another scheduled basis, or on an event driven basis in response to a particular event according to the particular requirements of a given situation. In the illustrative embodiments, the malicious code detection program includes instructions for the information handling system to examine characteristics and behaviors of the information handling system's instructions and/or data.

[0032] The malicious code detection program includes instructions for the information handling system to evaluate the information handling system's instructions and/or data to determine whether such instructions and/or data are valid code (i.e., non-malicious) or malicious code or any one or more types. The malicious code detection program includes respective detection routines, sets of weights, and weighted scoring algorithms for detecting one or more types of valid code and/or one or more types of malicious code.

[0033] The malicious code detection program **40** contains detection routines **42**, including valid program detection routines **52** and malicious code detection routines **54**. The valid program detection routines **52** include one or more routines identified by $v_1, v_2, v_3, \dots, v_M$ in **FIG. 2**. The valid program detection routines **52** are configured to determine whether the program under investigation has characteristics and behaviors usually associated with a valid program. The malicious code detection routines **54** include one or more routines identified by $t_1, t_2, t_3, \dots, t_N$ in **FIG. 2**. The malicious code detection routines **54** are configured to determine whether the program under investigation has characteristics and behaviors usually associated with a malicious code program.

[0034] In one embodiment, the valid program detection routines **52** and the malicious code detection routines **54** are configured to gather a variety of characteristic and behavior information from the information handling system in a variety of ways, such as: (a) examining the program itself; (b) accessing information from the operating system **46** using application programming interfaces (APIs) **48** to the operating system (including documented APIs and/or undocumented API's); (c) kernel and/or device driver interfacing; and/or (d) direct access to resources of the information handling system such as memory, network connections, storage media, and/or other devices. For example, as shown in **FIG. 2**, the detection routines **42** gather such information by examining one or more of (a) a binary image **60** or (b) a library or other information (e.g., tables showing a program's network connection activity) that indicates the aforementioned characteristics and behaviors, such as process behavior information **50**.

[0035] For example, a detection routine **42** can be configured to account for the following. Many trojans, keyloggers, remote controls and monitoring software programs log keystrokes on the innocent victim's computer and transmit the

keystroke information from the innocent victim's computer to the evil hacker's computer. In one embodiment, a malicious code detection routine **54** determines whether the program being examined is logging keystrokes. Since there are many different ways for a program to log keystrokes, one or more of the malicious code detection routines **54** can be configured to examine the program under investigation to determine whether the program is using any of a number of different mechanisms for logging keystrokes. Detection routines may output many different types of results, such as numeric values, boolean values, counts or lists.

[0036] The malicious code detection program **40** further includes a scoring algorithm **44**. In the illustrative embodiment, the scoring algorithm calculates two scores, namely a valid program score **56** and a malicious code score **58**. In an alternative embodiment, the scoring algorithm calculates the valid program score **56**, but not the malicious code score **58**. In another alternative embodiment, the scoring algorithm calculates the malicious code score **58**, but not the valid program score **56**.

[0037] If the result of a valid program detection routine **52** indicates that the characteristic or behavior of the program being examined was that of a valid program, then a weight, W_i , is associated with the routine and that weight contributes positively to the valid program score **56**. A weight, W_i , is assigned to each valid program detection routine, for $i=1$ to M , where M is the number of the valid program detection routine.

[0038] The weight indicates (a) the detection routine's importance, (b) the extent to which the particular behavioral trait being measured by the detection routine is present, and (c) the extent to which the behavioral trait contributes to the determination of whether the program is valid or malicious. To determine the value that results from combining the weight with the results of the detection routine, the information handling system performs any one or more of a variety of operations, such as performing an arithmetic or algebraic operation on the combination of the weight and the result of the detection routine or simply assigning the combination a numerical value.

[0039] If the result of a malicious code detection routine **54** indicates that the characteristic or behavior of the program being examined was that of a malicious code program, then a weight, W_j , is associated with the routine and that weight contributes positively to the malicious code score **58**. A weight, W_j , is assigned each malicious code detection routine, for $j=1$ to N , where N is the number of the malicious code detection routine.

[0040] According to one embodiment, the scoring algorithm **44** includes an algorithm that has an algebraic formula for determining the two scores **56** and **58**. The scoring algorithm is dependent on the valid program detection routines **52** and the weights, W_i , associated with each valid program detection routine, in addition to, the malicious code detection routines **54** and the weights W_j , associated with each malicious code detection routine. The algebraic formula or equation can also be made arbitrarily complex (e.g., associating additional weights to one or more to combinations of detection routines **42**).

[0041] In one embodiment, the scoring algorithm **44** includes an algebraic equation defined as a sum of weighted