

87. The information handling system of claim 77, wherein execution of the MCDC occurs in response to at least one of the following: a random initiation, an event driven initiation, and a periodic initiation.

88. The information handling system of claim 77, wherein the malicious code includes a trojan horse.

89. The information handling system of claim 77, wherein the malicious code includes remote control software.

90. The information handling system of claim 77, wherein the malicious code includes a keystroke logger.

91. The information handling system of claim 77, wherein the malicious code includes spyware.

92. The information handling system of claim 77, wherein the malicious code includes a worm.

93. The information handling system of claim 77, wherein the malicious code includes a virus.

94. The information handling system of claim 77, wherein the malicious code includes monitoring software.

95. 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 code under investigation, the detection routines associating weights to respective code under investigation in response to detections of malicious code as a function of the detection routines; and

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

96. The method of claim 95, wherein the applying comprises:

applying the detection routines to gather information about the code under investigation by at least one of the following: examining the code under investigation; and

searching for information in the information handling system about the code under investigation.

97. The method of claim 95, wherein determining whether the code under investigation is malicious code includes scoring the execution of the detection routines as a function of the weights, wherein scoring includes configuring a scoring algorithm to identify the code under investigation as malicious code in response to a malicious code score.

98. The method of claim 95, wherein the malicious code includes a trojan horse.

99. The method of claim 95, wherein the malicious code includes remote control software.

100. The method of claim 95, wherein the malicious code includes a keystroke logger.

101. The method of claim 95, wherein the malicious code includes spyware.

102. The method of claim 95, wherein the malicious code includes a worm.

103. The method of claim 95, wherein the malicious code includes a virus.

104. The method of claim 95, wherein the malicious code includes monitoring software.

* * * * *