

What is claimed is:

1. A method for detecting malware, the method being implemented by a processor on a computing device, the method comprising:
 - receiving, by the processor, a request for a first web page;
 - determining, by the processor, at least one expected attribute of the first web page;
 - generating, by the processor, a modified web page by combining the first web page with a predetermined set of code, the predetermined set of code being configured to detect whether the malware is present on a client device;
 - transmitting, to the client device, the modified web page;
 - receiving, from the client device, data collected from an executed version of the modified web page;
 - determining, by the processor, at least one attribute of the executed version of the modified web page;
 - comparing, by the processor, the at least one expected attribute of the first web page with the at least one attribute of the executed version of the modified web page; and
 - determining, by the processor, whether the malware is present on the client device based on a result of the comparing.
2. The method of claim 1, further comprising transmitting, to the client device, an alert message indicating that the malware is present on the client device.
3. The method of claim 1, wherein the at least one expected attribute of the first web page includes a first number of JavaScript elements that are associated with the first web page, and wherein the determining whether the malware is present on the client device further comprises comparing the first number of JavaScript elements with a second number of JavaScript elements that are associated with the executed version of the modified web page.
4. The method of claim 1, wherein the at least one expected attribute of the first web page includes a first set of identifiers that correspond to JavaScript elements that are associated with the first web page, and wherein the determining whether the malware is present on the client device further comprises comparing the first set of identifiers with a second set of identifiers that correspond to JavaScript elements that are associated with the executed version of the modified web page.

5. The method of claim 1, wherein the at least one expected attribute of the first web page includes a first set of sources of JavaScript elements that are associated with the first web page, and wherein the determining whether the malware is present on the client device further comprises comparing the first set of sources with a second set of sources of JavaScript elements that are associated with the executed version of the modified web page.

6. The method of claim 1, wherein the at least one expected attribute of the first web page includes a first set of Uniform Resource Identifiers (URIs) that are associated with the first web page, and wherein the determining whether the malware is present on the client device further comprises comparing the first set of URIs with a second set of URIs that are associated with the executed version of the modified web page.

7. The method of claim 1, wherein the at least one expected attribute of the first web page includes a first set of JavaScript function names that are associated with the first web page, and wherein the determining whether the malware is present on the client device further comprises comparing the first set of JavaScript function names with a second set of JavaScript function names that are associated with the executed version of the modified web page.

8. The method of claim 1, wherein the at least one expected attribute of the first web page includes first information that relates to JavaScript event handlers that are associated with the first web page, and wherein the determining whether the malware is present on the client device further comprises comparing the first information with second information that relates to JavaScript event handlers that are associated with the executed version of the modified web page.

9. The method of claim 1, wherein the at least one expected attribute of the first web page includes a first set of cookies that are associated with the first web page, and wherein the determining whether the malware is present on the client device further comprises comparing the first set of cookies with a second set of cookies that are associated with the executed version of the modified web page.

10. The method of claim 1, further comprising:
when a determination is made that malware is not present on the client device, storing information that relates to the first web page and the client device in a first database; and

when a determination is made that malware is present on the client device, storing information that relates to the first web page, the client device, and the malware in a second database.

11. A computing device configured to implement an execution of a method for detecting malware, the computing device comprising:

- a display screen;

- a processor;

- a memory; and

- a communication interface coupled to each of the processor, the memory, and the display screen,

- wherein, when the method is being executed, the processor is configured to:

- receive, via the communication interface, a request for a first web page;

- determine at least one expected attribute of the first web page;

- generate a modified web page by combining the first web page with a predetermined set of code, the predetermined set of code being configured to detect whether the malware is present on a client device;

- transmit, to the client device via the communication interface, the modified web page;

- receive, from the client device via the communication interface, data collected from an executed version of the modified web page;

- determine at least one attribute of the executed version of the modified web page;

- compare the at least one expected attribute of the first web page with the at least one attribute of the executed version of the modified web page; and

- determine whether the malware is present on the client device based on a result of the comparison.

12. The computing device of claim 11, wherein the processor is further configured to transmit, to the client device via the communication interface, an alert message indicating that the malware is present on the client device.

13. The computing device of claim 11, wherein the at least one expected attribute of the first web page includes a first number of JavaScript elements that are associated with the first web page, and wherein the processor is further configured to determine whether the malware is present on the client device by comparing the first number of JavaScript elements with a second

number of JavaScript elements that are associated with the executed version of the modified web page.

14. The computing device of claim 11, wherein the at least one expected attribute of the first web page includes a first set of identifiers that correspond to JavaScript elements that are associated with the first web page, and wherein the processor is further configured to determine whether the malware is present on the client device by comparing the first set of identifiers with a second set of identifiers that correspond to JavaScript elements that are associated with the executed version of the modified web page.

15. The computing device of claim 11, wherein the at least one expected attribute of the first web page includes a first set of sources of JavaScript elements that are associated with the first web page, and wherein the processor is further configured to determine whether the malware is present on the client device by comparing the first set of sources with a second set of sources of JavaScript elements that are associated with the executed version of the modified web page.

16. The computing device of claim 11, wherein the at least one expected attribute of the first web page includes a first set of Uniform Resource Identifiers (URIs) that are associated with the first web page, and wherein the processor is further configured to determine whether the malware is present on the client device by comparing the first set of URIs with a second set of URIs that are associated with the executed version of the modified web page.

17. The computing device of claim 11, wherein the at least one expected attribute of the first web page includes a first set of JavaScript function names that are associated with the first web page, and wherein the processor is further configured to determine whether the malware is present on the client device by comparing the first set of JavaScript function names with a second set of JavaScript function names that are associated with the executed version of the modified web page.

18. The computing device of claim 11, wherein the at least one expected attribute of the first web page includes first information that relates to JavaScript event handlers that are associated with the first web page, and wherein the processor is further configured to determine whether the malware is present on the client device by comparing the first information with

second information that relates to JavaScript event handlers that are associated with the executed version of the modified web page.

19. The computing device of claim 11, wherein the at least one expected attribute of the first web page includes a first set of cookies that are associated with the first web page, and wherein the processor is further configured to determine whether the malware is present on the client device by comparing the first set of cookies with a second set of cookies that are associated with the executed version of the modified web page.

20. The computing device of claim 1, wherein:

when a determination is made that malware is not present on the client device, the processor is further configured to store, in the memory, information that relates to the first web page and the client device in a first database; and

when a determination is made that malware is present on the client device, the processor is further configured to store, in the memory, information that relates to the first web page, the client device, and the malware in a second database.