CLAIMS

1. A method for restoring a web site in the event of a hack or a defacement, the website comprising at least one webpage having at least one functional element, the method comprising the steps of: copying the at least one webpage of the website with the at least one functional element to create a replicated web site on a restorer server, the at least one functional element of the replicated website capable of accepting user input to trigger an event; creating at the restorer server, a secure website replica from the replicated website by deactivating the at least one functional element rendering the secure website replica incapable of accepting user input to trigger the event by at least one of removing or disabling the at least one functional element of the replicated website; presenting the secure website replica in place of the website once the hack or the defacement of the website has been detected; and redirecting web traffic from the website to the secure website replica.

2. The method of claim 1 wherein the event is any one of the following: the restorer server accessing an information sensitive database, the restorer server displaying an error message on the replicated website, a client machine downloading files and a redirection to another universal resource locator (URL).

3. The method of claim 1 wherein the at least one deactivated functional element is any one of the following: a javascript, an input field, a text area, a form, a select tag, a button, an anchor link, an image and a hyperlink.

4. The method of claim 1 further comprising the step of removing at least one embedded element from the secure website replica.

5. The method of claim 4 wherein the at least one embedded element is any one of the following: an IFrame, an applet tag, an object tag and an XML tag.

6. The method of claim 1 further comprising the step of disabling at least one cascading style sheet on the secure website replica.

7. The method of claim 1 further comprising the step of preventing a client browser from caching the secure website replica.

8. The method of claim 1 wherein the hack or the defacement of the website is detected by a defacement detection engine.

9. The method of claim 8 wherein the step of redirecting with the defacement detection engine, web traffic from the website to the secure website replica comprises the step of updating a record in a domain name server to replace an internet protocol (IP) address of a web server hosting the website, with an IP address of the restorer server.

10. The method of claim 8 wherein the step of redirecting with the defacement detection engine, web traffic from the website to the secure website replica comprises the step of updating a rule set of a load balancer.

11. The method of claim 8 wherein the step of redirecting with the defacement detection engine, web traffic from the website to the secure website replica comprises the step of blocking web traffic to a web server hosting the website and allowing web traffic to the restorer server.

12. The method of claim 1 further comprising the step of crawling the website with the restorer server to identify the at least one webpage of the website to be copied.

13. The method of claim 12 further comprising the step of providing a web portal to an organization to allow the organization the ability to customize the deactivation of the at least one functional element, and schedule and initiate the steps of crawling the website, copying the at least one webpage of the website, creating a secure website replica and redirecting web traffic from the website to the secure website replica.

14. A system for restoring a website in the event of a hack or a defacement, the website comprising at least one webpage having at least one functional element, the system comprising a

restorer server having a processor and a memory, the restorer server configured to: copy the at least one webpage of the website with the at least one functional element to create a replicated website on a restorer server, the at least one functional element of the replicated website capable of accepting user input to trigger an event; create a secure website replica from the replicated website by deactivating the at least one functional element rendering the secure website replica incapable of accepting user input to trigger the event by at least one of removing or disabling the at least one functional element of the replicated web site; present the secure website replica in place of the website once the hack or the defacement of the website has been detected; and redirect web traffic from the website to the secure website replica.

15. The system of claim 14 wherein the event is any one of the following: the restorer server accessing an information sensitive database, the restorer server displaying an error message on the replicated website, a client machine downloading files and a redirection to another universal resource locator (URL).

16. The system of claim 14 wherein the at least one deactivated functional element is any one of the following: a javascript, an input field, a text area, a form, a select tag, a button, an anchor link, an image and a hyperlink.

17. The system of claim 14 wherein the restorer server is further configured to remove at least one embedded element from the secure website replica.

18. The system of claim 17 wherein the at least one embedded element is any one of the following: an IFrame, an applet tag, an object tag and an XML tag.

19. The system of claim 14 wherein the restorer server is further configured to disable at least one cascading style sheet on the secure website replica.

20. The system of claim 14 wherein the restorer server is further configured to prevent a client browser from caching the secure website replica.

21. The system of claim 14 further comprising a defacement detection engine for detecting that the website has been hacked or defaced.

22. The system of claim 21 wherein the defacement detection engine redirects web traffic from the website to the secure website replica by updating a record in a domain name server to replace an internet protocol (IP) address of a web server hosting the website, with an IP address of the restorer server.

23. The system of claim 21 wherein the defacement detection engine redirects web traffic from the website to the secure website replica by updating a rule set of a load balancer.

24. The system of claim 21 wherein the defacement detection engine redirects web traffic from the website to the secure website replica by blocking web traffic to a web server hosting the website and allowing web traffic to the restorer server.

25. The system of claim 14 wherein the restorer server is further configured to crawl the website to identify the at least one webpage of the website to be copied.

26. The system of claim 25 further comprising a web portal for allowing an organization the ability to customize the deactivation of the at least one functional element, and schedule and initiate the restorer server to crawl the website, copy the at least one webpage of the website and create a secure website replica, and the defacement detection engine to redirect web traffic from the website to the secure website replica.

27. A computer program product for restoring a website in the event of a hack or a defacement, the website comprising at least one webpage having at least one functional element, the computer program product having a non-transitory computer readable storage medium having computer readable program code operable on a restorer server having a processor and a memory, the computer readable program code configured to: copy the at least one webpage of the website with the at least one functional element to create a replicated website on a restorer server, the at least one functional element of the replicated website capable of accepting user input to trigger

an event; create a secure website replica from the replicated website by deactivating the at least one functional element rendering the secure website replica incapable of accepting user input to trigger the event by at least one of removing or disabling the at least one functional element of the replicated web site; present the secure website replica in place of the website once the hack or the defacement of the website has been detected; and redirect web traffic from the website to the secure website replica.