CLAIMS

1. A computer-implemented method for preventing an activity of a malware application in a computer system, the method being executable by a processor of the computer system, the method comprising:

receiving, by the processor, at least one artefact that is indicative of an execution of a sandbox environment in the computer system, the sandbox environment including a virtual machine;

causing, by the processor, installation of the at least one artefact of the sandbox environment in the computer system for simulating the sandbox environment in the computer system without actually executing the sandbox environment;

receiving, by the processor, an indication of at least one interaction of a given application with the at least one artefact;

analyzing, by the processor, an activity of the given application to detect at least one of a first type event and a second type event triggered thereby after executing the at least one interaction,

the first type event being the given application aborting execution of any activity after the at least one interaction with the at least one artefact; and

the second type event being the given application executing the activity thereof in a manner different from a predetermined manner of executing the activity associated with the given application;

in response to the analyzing rendering a positive result:

identifying the given application as being the malware application; and

using data indicative of a digital footprint of the given application in the computer system for updating the at least one artefact for further preventing the activity of the malware application.

2. The method of claim 1, wherein the at least one artefact comprises at least one of:
one or more files to be created at predetermined paths in the system;

one or more language packs to be added to the computer system without adding corresponding keyboard layouts;

one or more idle network interfaces with names, IP, and MAC addresses having predetermined names to be generated in the computer system;

one or more idle processes to be launched at predetermined paths and under predetermined names;

one or more predetermined keys to be added in a system register of the computer system;

one or more predetermined respective interface elements to be generated and added to at least one of a launch menu and a quick launch panel of the computer system; and

one or more environment variables associated with the sandbox environment to be registered with the computer system.

3. The method of claim 1, wherein the at least one artifact is one of:

an active artefact configured to interact with at least one application running in the computer system; and

a passive artefact incapable of interacting with any application running therein.

4. The method of claim 1, wherein the analyzing further comprises determining if the given application is the malware application, the determining including at least one of: searching for the given application on one of a whitelist and a blacklist of applications; determining if a predetermined respective weight of the at least one artefact, associated with triggering the at least one of the first type event and the second type event, exceeds a predetermined weight threshold; and determining at least one difference in behaviors of the given application in the sandbox environment and in the computer system.

5. The method of claim 1, further comprising transmitting, via a communication network, the data indicative of the digital footprint of the given application to an analysis and update server, the transmitting being executed in an encrypted form.

6. The method of claim 5, wherein the analysis and update server is configured to execute at least one of:

analyzing the digital footprint of the given application;

adding the at least one artefact to an artifact database associated with the sandbox environment; and

transmitting updates of the artifact database to the computer system.

7. The method of claim 1, wherein the at least one artifact is being updated based on monitoring data from at least one of the following subsystems: a file system, a list of running processes, and a registry; and the method further comprises updating a status of the at least one artifact, the status including at least one of: adding, removing, and modifying.

8. The method of claim 5, wherein the receiving of the at least one artefact is from the analysis and update server.

9. A computer system for preventing an activity of a malware application therein, the computer system including:

a processor;

a non-transitory computer-readable memory storing instructions;

the processor, upon executing the instructions, being configured to:

receive at least one artefact that is indicative of an execution of a sandbox environment in the computer system, the sandbox environment including a virtual machine;

cause installation of the at least artefact of the sandbox environment in the computer system for simulating the sandbox environment in the computer system without actually executing the sandbox environment,

receive an indication of at least one interaction of a given application with the at least one artefact;

analyze an activity of the given application to detect at least one of a first type event and a second type event triggered thereby after executing the at least one interaction,

the first type event being the given application aborting execution of any activity after the at least one interaction with the at least one artefact; and

the second type event being the given application executing the activity thereof in a manner different from a predetermined manner of executing the activity associated with

the given application;

in response to analyzing rendering a positive result:

identify the given application as being the malware application; and

use data indicative of a digital footprint of the given application in the computer system for updating the at least one artefact for further preventing the activity of the malware application.

10. The computer system of claim 9, wherein the at least one artefact comprises at least one of:

one or more files to be created at predetermined paths in the system;

one or more language packs to be added to the computer system without adding corresponding keyboard layouts;

one or more idle network interfaces with names, IP, and MAC addresses having predetermined names to be generated in the computer system;

one or more idle processes to be launched at predetermined paths and under predetermined names;

one or more predetermined keys to be added in a system register of the computer system;

one or more predetermined respective interface elements to be generated and added to at least one of a launch menu and a quick launch panel of the computer system; and

one or more environment variables associated with the sandbox environment to be registered with the computer system.

11. The computer system of claim 9, wherein the at least one artifact is one of:

an active artefact configured to interact with at least one application running in the computer system; and

a passive artefact incapable of interacting with any application running therein.

12. The computer system of claim 9, wherein the processor, configured to analyze the activity of the given application, is further configured to determine if the given application is the

malware application, by executing at least one of: searching for the given application on one of a whitelist and a blacklist of applications; determining if a predetermined respective weight of the at least one artefact, associated with triggering the at least one of the first type event and the second type event, exceeds a predetermined weight threshold; and determining at least one difference in behaviors of the given application in the sandbox environment and in the computer system.

13. The computer system of claim 9, wherein the processor is further configured to transmit, via a communication network, in an encrypted form, the data indicative of the digital footprint of the given application to an analysis and update server.

14. The computer system of claim 13, wherein the analysis and update server is configured to execute at least one of:

analyzing the digital footprint of the given application;

adding the at least one artefact to an artifact database associated with the sandbox environment; and

transmitting updates of the artifact database to the computer system.

15. The computer system of claim 9, wherein the at least one artifact being updated based on monitoring data from at least one of the following subsystems: a file system, a list of running processes, and a registry; and the processor is further configured to update a status of the at least one artifact, the status including at least one of: adding, removing, and modifying.

16. The computer system of claim 13, wherein the processor is configured to receive the at least one artefact from the analysis and update server.