

ABSTRACT

A method and a system for preventing an activity of a malware application in a computer system are provided. The method comprising: receiving at least one artefact of a sandbox environment to be installed in the computer system for simulating the sandbox environment in the computer system; receiving an indication of at least one interaction of a given application with the at least one artefact; analyzing 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; 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 further updating the at least one artefact for further preventing the activity of the malware application.

Fig. 1