

ABSTRACT

A method and a system for detecting malware activity in a .NET platform are provided. The method comprises: determining an architecture of the .NET platform; modifying contents of a given .NET method by adding thereto an executable payload, thereby generating a respective modified .NET method, the executable payload being configured for logging and storing data of current activities in the .NET platform; storing the respective modified .NET method in the .NET platform; in response to calling, by a .NET application, the respective modified .NET method: executing the executable payload to cause the logging the current activity in the .NET platform to generate an activity log; and transmitting the activity log for analysis to determine presence of the malware activity in the .NET platform.

Fig. 1