Malware Windows Evasifs : Impact sur les Antivirus et Possible Contremesure

Cédric Herzog[1], Valérie Viet Triem Tong[1], Pierre Wilke[1], and Jean-Louis Lanet[1]

[1]Inria, CentraleSupélec, Univ Rennes, CNRS, IRISA, Rennes, France
{firstname.lastname}@inria.fr

Résumé.

Ce papier vise à déterminer les possibilités pour un malware de détecter les antivirus puis, à évaluer l'efficacité de ces techniques sur un ensemble d'antivirus parmi les plus populaires de cette année. Nous proposons par la suite une contremesure visant à stopper ce genre de malware en simulant les modifications faites par un AV dans le système d'exploitation. Ces leurres sont créés via l'instrumentation de l'API Windows à l'aide de Microsoft Detours. Nous évaluerons cette contremesure sur quelques exemples de malwares évasifs récupérées dans la nature. Une partie des résultats a été présentée dans la conférence SECRYPT 2020.

Mots clés :
Antivirus; Evasion; Windows Malware; Windows API;