Camouflage in Malware : from encryption to metamorphism

Abstract

Camouflage of malware is a serious challenge for antivirus experts and code analysts. Malware use various techniques to camouflage them to not be easily visible and make their lifetime as longer as possible. Although, camouflage approaches cannot fully stop the analyzing and fighting against the malware, but it make the process of analyzing and detection prolonged, so the malware can get more time to widely spread. It is very important for antivirus technologies to improve their products by shortening the detection procedure, not only at the first time facing with a new threat, but also in the future detections. In this paper, we intend to review the concept of camouflage in malware and its evolution from non-stealth days to modern metamorphism. Moreover, we explore obfuscation techniques exploited by metamorphism, the most recent method in malware camouflage.