The devil’s right hand: An investigation on malware-oriented obfuscation techniques

Reza Hedayat

Abstract:

Malicious software, also known as malware, represents the profitable art of destruction as it is able to do any kind of harm to a system in a stealthy manner as well as to hide its existence. Furthermore, its rise has prevailed and there is no end sight. When it comes to its great success, it is its most valuable member and right hand, which is mainly responsible for this achievement, namely obfuscation. Obfuscation techniques are applied to protect assets of malware with regards to confidentiality, integrity and availability for a limited time.

In this work, we investigate on malware-oriented obfuscation techniques by analysing its origins, the state-of-the-art techniques, its future trends and also how to evaluate its effectiveness. The contribution of this work is thereby threefold:

1. Malware-oriented Obfuscation primitives
   A novel method is proposed to categorise malware-oriented obfuscation layers based on predefined primitives, which have been retrieved via research work and hands-on dissection of real malware samples.

2. Next Generation Obfuscation
   In order to be able to keep pace with the threats of tomorrow, it is of paramount importance to get to know how they will look like. Therefore, predictions concerning possible directions of malware-oriented obfuscation techniques are made and discussed.

3. MOVE Framework
   The proposed framework is based on an empirical model and allows to measure the effectiveness of malware-oriented obfuscation techniques in evading anti-malware solutions. Moreover, a prototype has also been implemented in order to demonstrate the framework’s feasibility.