Analysis of known and unknown malware bypassing techniques

ABSTRACT

Nowadays, malware attacks are the most expensive damages for organizations in different types of computer and network systems. While different types of attacks are well surveyed and documented, little details related to bypass malware detections and defenses are provided in the public domains. Malware caused different types of attacks such as denial of service (DoS) attacks,business espionage, extorting money, etc. Therefore, implementing malware defenses for organizations' internal networks are uttermost important.In this paper, bypassing the well-known and unknown malware through the host-based Anti Viruses (AVs) that are based on signature detection is illustrated, and it is shown that how even a known malware might be bypassed anti viruses and firewalls to be executed in organizations' internal computer networks. Right after that, an unknown malware detection system to protect organization's internal networks from unknown and known malware before they reach into the victims' systems is surveyed and provided.

Keyword: Malware defense; Bypassing malware; Penetration testing; Malware detection