Investigation of bypassing malware defences and malware detections

ABSTRACT

Nowadays, malware incident is one of the most expensive damages caused by attackers. Malwares are caused different attacks, so considerations and implementations of malware defences for internal networks are important.

In this papers, different techniques such as repacking, reverse engineering and hex editing for bypassing host-based Anti Virus (AV) signatures are illustrated, and the description and comparison of different channels and methods when malware might reach the host from outside the networks are demonstrated. After that, bypassing HTTP/SSL and SMTP malware defences as channels are discussed. Finally, as it is important to find and detect new and unknown malware before the malware gets in to the victims, a new malware detection technique base on honeynet systems is surveyed.

Keyword: Malware defences; Bypassing malware; Honeynet; Anti viruses; Penetration testing