A Utility-Based Sequential Approach for ELF Malware Analysis

Mohammed Rauf Ali Khan[1]

[1]LTIMindtree Limited

March 07, 2024

Abstract

The demand for various unix/ linux based systems is high. Several IoT appliances are usually based on linux. These operating systems have uncountable applications and offer several utilities to their users. Several Advanced Persistent Threats have therefore increased the rate of attacks on such platforms. There is a high rise in malicious entities that are intended to have harmful effects towards linux environments. Varieties of trojans, spyware and ransomware of executable and linkable format have been seen in recent times. These malware majorly target linux based systems. A generic approach that can help malware researchers to perform static, dynamic and code analysis in a convenient way has been proposed. A sequential flow of processes beginning from static analysis, moving to behavioral analysis and then to code was provided. There are several utilities that pre-exist in linux based environments. These utilities can help one to gain several identities of compromise. It is important to detect and block such malware. Hence, there is a need to identify strings, behavioral patterns, code and persistence mechanisms they use. From helping a researcher to identify the file type, to writing YARA and SNORT rules for detecting those files using SIEMs, these linux utilities provide high level of support.