Journal of Computer Science Engineering and Information Technology Research (JCSEITR)
ISSN(P): 2250-2416; ISSN(E): Applied
Vol. 5, Issue 1, Jun 2015, 7-20
TJPRC Pvt. Ltd.

DEFENDING AGAINST MALWARES: SANDBOX DETECTION AND PREVENTION OF MALWARES IN ANDROID DEVICES

BABYSYLA. L[1], SATHEESH KUMAR. S[2] & SHAMEEDHA BEGUM. B[3]

[1]Department of CSE, National Institute of Technology, Tiruchirappalli, Tamil Nadu, India

[2]Senior Engineer, Cyber Forensics, CDAC, Thiruvananthapuram, Kerala, India

[3]Assistant Professor, CSE National Institute of Technology, Tiruchirappalli, Tamil Nadu, India

ABSTRACT

Nowadays, Android malwares are growing rapidly due to its wide popularity and openness. Malware authors inject malicious code into app and upload it into Play store or third party markets. Once it is installed in the Android device, it may cause severe threats such as financial loss, privacy leakage to users etc. Therefore, this project aims at implementing an Android application sandbox system with the intent to provide an initial understanding of the behavior of unknown packages through analysis during runtime.

This project is carried out as part of M.Tech Thesis work in Cyber Forensics, CDAC, Trivandrum. The proposed system executes the app under test in a sandbox environment and gives a detailed report about its behavior during runtime. In addition, a system is developed which can prevent applications from leaking privacy-sensitive data by restricting the categories of data an application can access.

KEYWORDS: Threat, Static Analysis, Sandboxes, Data Leakage, Monitoring API Calls, Restrict Permissions, Fake Data