The rise of obfuscated Android malware and impacts on detection methods

By: Elsersy, WF (Elsersy, Wael F.) [1] ; Feizollah, A (Feizollah, Ali) [1] ; Anuar, NB (Anuar, Nor Badrul) [1]

PEERJ COMPUTER SCIENCE

Volume: 8

Article Number: e907

DOI: 10.7717/peerj-cs.907

Published: MAR 9 2022

Indexed: 2022-04-02

Document Type: Article

Abstract

The various application markets are facing an exponential growth of Android malware. Every day, thousands of new Android malware applications emerge. Android malware hackers adopt reverse engineering and repackage benign applications with their malicious code. Therefore, Android applications developers tend to use state-of-the-art obfuscation techniques to mitigate the risk of application plagiarism. The malware authors adopt the obfuscation and transformation techniques to defeat the anti-malware detections, which this paper refers to as evasions. Malware authors use obfuscation techniques to generate new malware variants from the same malicious code. The concern of encountering difficulties in malware reverse engineering motivates researchers to secure the source code of benign Android applications using evasion techniques. This study reviews the state-of-the-art evasion tools and techniques. The study criticizes the existing research gap of detection in the latest Android malware detection frameworks and challenges the classification performance against various evasion techniques. The study concludes the research gaps in evaluating the current Android malware detection framework robustness against state-of-the-art evasion techniques. The study concludes the recent Android malware detection-related issues and lessons learned which require researchers' attention in the future.

Keywords

Author Keywords: Android malware; Android security; Evasion techniques; Machine learning; Obfuscation techniques

Keywords Plus: DEEP LEARNING-METHOD; HYBRID APPROACH; SYSTEM; FEATURES; CODE; SIGNATURE; FRAMEWORK; ANALYZER; ATTACKS; THREAT

Author Information

Corresponding Address : Elsersy, Wael F.; Anuar, Nor Badrul (corresponding author)

Univ Malaya, Dept Comp Syst & Technol, Fac Comp Sci & Informat Technol, Kuala Lumpur, Wilayah Perseku, Malaysia

Addresses:
[1] Univ Malaya, Dept Comp Syst & Technol, Fac Comp Sci & Informat Technol, Kuala Lumpur, Wilayah Perseku, Malaysia

E-mail Addresses: wfarouk@siswa.um.edu.my; badrul@um.edu.my

Categories/Classification

Research Areas: Computer Science

Funding

Funding agency	Grant number
Fundamental Research Grant Scheme under the Ministry of Education Malaysia	FRGS/1/2018/ICT03/UM/02/3

Funding Table

View funding text

+ See more data fields

Journal information

PEERJ COMPUTER SCIENCE
eISSN: 2376-5992
Current Publisher: PEERJ INC, 341-345 OLD ST, THIRD FLR, LONDON EC1V 9LL, ENGLAND
Research Areas: Computer Science
Web of Science Categories: Computer Science, Artificial Intelligence; Computer Science, Information Systems; Computer Science, Theory & Methods

1.392
Journal Impact Factor ™ (2020)

237 Cited References

Showing 30 of 237 View as set of results

(from Web of Science Core Collection)