UTS UNIVERSITY OF TECHNOLOGY SYDNEY

Analysis of the Latest Trojans on Android Operating System

by Baodi Ning

Thesis submitted in fulfilment of the requirements for the degree of

Master of Analytics

under the supervision of Dr. Yulei Sui
and co-supervision of Dr. Jingling Xue

University of Technology Sydney
Faculty of Engineering and Information Technology

January 2021

CERTIFICATE OF ORIGINAL AUTHORSHIP

I, Baodi Ning declare that this thesis, is submitted in fulfilment of the requirements for the award of Master of analytics, in the Faculty of Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Signature: Production Note:
Signature removed prior to publication.

Date: January 6th, 2021

Abstract

With the rapid advancements of electronics, the mobile operating system can accommodate various applications, which greatly facilitates people's everyday life. With a user group of more than 2 billion, the Android platform provides a diverse ecosystem for developing and publishing all sorts of applications. Although Google's official application store, Google Play, contains over 2 million apps, such a huge market also attracts hackers to make profits through distributing malware.

Mobile malware has rocketed since 2009. As reported by Broadcom Inc., an industry-leading security company, 2017 witnessed an increase of new mobile malware strains, compared with the year of 2016. Additionally, more profit-driven malware emerged with the growth of underground markets. Due to the fragmentation problem of the Android platform, Android has long been the most targeted operating system suffering from attacks. To keep pace with the cutting-edge anti-malware countermeasures adopted by cyber-security businesses, malware developers have abused high-level obfuscation, virtual environment recognition, conditional execution (logic bomb), run-time payload dropping, etc., to fool their opponents (i.e., security defending products and reverse engineering tools). These techniques are usually more obvious to trace during the evolution and diversification of a malware family. In this thesis, we take a close look into both recent Android trojans and one specific family of Android banking trojan, that infiltrates banking applications to steal credentials or trick victims to type in their usernames and passwords through displaying fake login interfaces. This thesis focuses on both statically reverse engineering the samples and dissecting the programs to understand their internal logic and find the similar features that could be used to assist security analysts, and dynamically monitor their behaviors in emulators. From public and private sources, 2380 samples of trojans from 20 (sub)families have been collected. As a result of the analysis, a lucid overview and improved apprehension of Android trojans are provided. The results indicate that Android trojans evolves towards possessing more malicious capabilities and more diverse permutations without losing their core design, which would cause more limitations and ineffectiveness for modern security solutions.

Acknowledgement

Throughout my research life pursuing a master's degree, I have received a lot of support from a wide range of people, both online and offline, some are friends or relatives while some have never been in contact.

First, I would like to sincerely thank my supervisor, Sui, whose expertise and resources are significant in both giving recommendations for revising the published articles as well as this thesis and informing possible journals and/or conferences to submit potentially publishable drafts. His insightful suggestions make my work more coherent and professional.

I would like to acknowledge my colleagues Guanqin Zhang, Zexin Zhong and Yanxin Zhang, who have helped me with reviewing drafts. I want to thank them all for their advice on perfecting the work to a higher level.

Also, I would like to thank some of the security professionals I have followed from Twitter, who are very resourceful and let me know many useful tools for both reverse engineering and analysis. Among them, @xabc0 a.k.a. Ahmet Bilal Can is the one that leads me into the world of banking trojans and malware analysis by his posts. @pr3wtd a.k.a. Witold Precikowski is the one who founded Apkdetect [1], and helped me with answering my questions when I encountered some weird code in the reverse-engineered source code. @LukasStefanko a.k.a. Lukas Stefanko also provided me with good ideas when I had some confusion when analyzing some malicious payloads of Bankbot Anubis.

In addition, I would like to thank my parents. I appreciate their encouragement when I felt frustrated or disappointed during my research. Their support made me through the plight. Moreover, this dissertation would not be completed without the company and communication from my friends, Wei Liu and Zhe, who have given me helpful suggestions and provided informative discussions based on their experiences of pursuing a PhD degree. Besides, the entertainment with them refreshed my mind from intensive research.

Finally, I would like to thank Bilibili as well as Youtube for providing records of great courses as well as amusing content for cheering and charging me up during my off-work hours.

Contents

List of Figures

List of Tables