COVID-19 Android Malware Detection Using Permissions and App Icons

David Tan
Mentor: Alfredo J. Perez
Columbus State University, TSYS School of Computer Science

Abstract

- In this paper, we proposed an Android permissions-based COVID-19 malware detection system that determines if an application is malicious based on the usage of suspicious permissions.
- Through extensive experiments, the proposed model has demonstrated a high level of symmetry between irrelevant permissions and malware applications.
- The proposed system has the potential to provide a low-cost alternative for Android malware detection for malicious applications including repacked applications.

Introduction

- Since the start of the COVID-19 pandemic in late 2019, there has been a dramatic increase in the percentage of malicious applications targeting mobile devices worldwide which indicates that malicious developers are capitalizing on the COVID-19 pandemic (see figure from "Beyond the Virus: A First Look at Coronavirus-themed Android Malware").
- These malicious Android applications, disguised as benign applications, are designed to either steal users' private information or make profit by phishing and extortion in the form of malware like worms, exploits, Trojans, and viruses.
- Android's status as one of most commonly used smartphone operating systems and its daily increase in applications in the smartphone application market has made the scope of this issue of increasingly emerging Android malware applications a pressing issue in the industry.

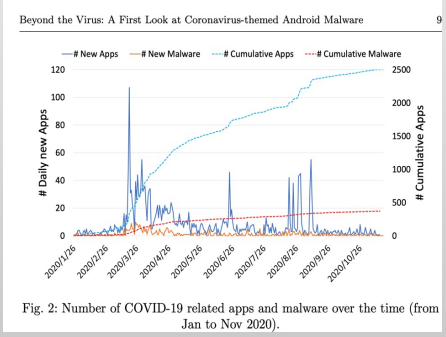

Fig. 2: Number of COVID-19 related apps and malware over the time (from Jan to Nov 2020).

Methodology

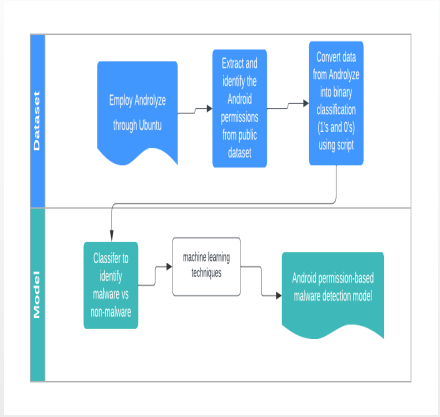

Fig. 1. shows an overview of our multi-level-based methodology to produce our Android permission-based malware model.

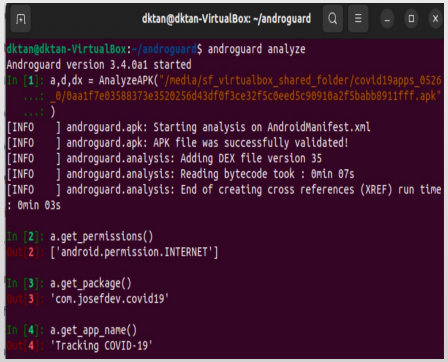

Fig. 2. shows the application of Androlyze, a Androguard tool, to analyze and evaluate the apk files from the public dataset of 2,017 applications from the paper "Beyond the Virus: A First Look at Coronavirus-themed Android Malware."

Results

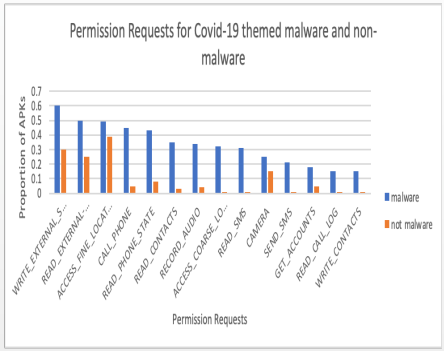

Fig. 3. "Permission Requests for COVID-19 themed malware and non-malware" presented similar results to those found in the paper "Beyond the Virus: A First Look at Coronavirus-themed Android Malware" which serves to validate our research and methodology.

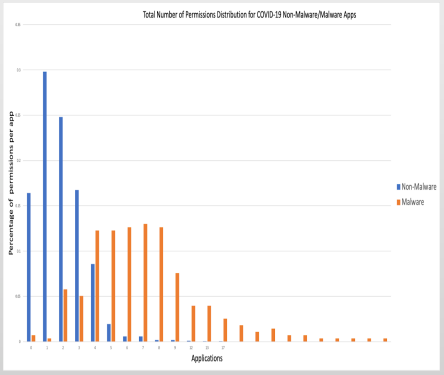

Fig. 4. "Total Number of Permissions Distribution for COVID-19 Non-Malware/Malware Apps" served the purpose of confirming the feasibility of our research goal to create an Android permissions-based COVID-19 malware detection system with machine learning technologies.

Conclusion

- In conclusion, the popularity and the ease of mobile application distribution have spurred the interest of many cyber-criminals across the globe.
- This interest has been further fueled by the COVID-19 pandemic, and since its start, there has been a dramatic increase in the percentage of malicious applications targeting mobile devices worldwide.
- With the purpose of providing an alternative for Android malware detection for malicious applications, we have proposed an Android permissions-based COVID-19 malware detection system.

Future Work

Due to the time constraint associated with a summer undergraduate research, we were not able to complete our second system of an icon-based COVID-19 malware detection system. Therefore, to further our research, we would develop this model in order to complete our novel contribution to the paper "Beyond the Virus: A First Look at Coronavirus-themed Android Malware."

References

- Wang L, He R, Wang H, Xia P, Li Y, Wu L, Zhou Y, Luo X, Sui Y, Guo Y, Xu G. (2021). Beyond the virus: a first look at coronavirus-themed Android malware. Empir Softw Eng. 26(4):82. doi: 10.1007/s10664-021-09974-4.
- Akbar, F., Hussain, M., Mumtaz, R., Riaz, Q., Wahab, A. W. A., & Jung, K.-H. (2022). Permissions-Based Detection of Android Malware Using Machine Learning. Symmetry (20738994), 14(4), N.PAG.
- Almomani, I., Alkhayer, A., & El-Shafai, W. (2022). An Automated Vision-Based Deep Learning Model for Efficient Detection of Android Malware Attacks. IEEE Access, Access, IEEE, 10, 2700–2720
- Hosseini, S., Nezhad, A. E., & Seilani, H. (2021). Android malware classification using convolutional neural network and LSTM. Journal of Computer Virology and Hacking Techniques, 17(4), 307–318.

Acknowledgements

I would like to thank Dr. Perez for guiding and helping me through this summer research. I would also like to thank Columbus State University and its faculty members and students along with my fellow REU participants.