Journal of Information Technology and Software Engineering

OPEN ACCESS Freely available online

Short Communication

Machine Learning for Identifying iOS Malware

Lisa Angelina[*]

Department of Computer Science, Heidelberg University, Baden-Württemberg, Germany

ABSTRACT

Smartphones have transformed into an indispensable component of our daily life. Smartphones are almost completely relied on as a communication tool, a source of information, and a source of pleasure on a social, political, and economic level. Rapid advances in information and cyber security have mandated particular attention to the privacy and security of smartphone data. Spyware detection systems have recently been created as a potential and appealing option for the privacy protection of smartphone users. Because the Android operating system is the most commonly used in the world, it is a major target for various groups interested in attacking smartphone users' privacy. This research presents a unique dataset gathered in a realistic setting using a novel data collecting approach based on a unified activity list.

The data is separated into three categories; Regular smartphone traffic, traffic data for the spyware installation procedure, and spyware operating traffic data. The random forest classification approach was used to verify this dataset and the suggested model. For data categorization, two approaches were used: binary-class classification and multi-class classification. In terms of precision, good results were obtained. The total average accuracy for binary-class classification was 79% and 77% for multi-class classification.

Keywords: Spyware; Machine learning; Spyware dataset

DESCRIPTION

Smartphones are quickly becoming an essential in daily life. By 2023, it is predicted that four billion people will be using smartphones. The Android operating system is the most widely used in the mobile device industry. It had 70% of the market in May 2021. Apple iOS controls 26.99 percent of the market, with other smaller vendors accounting for the remaining 3 percent [1,2].

Google Play is the official application store for Android handsets. It had around 2.9 million applications as of May 2021. AppBrain classifies 2.5 million as "regular applications" and the remaining 0.4 million as "low-quality apps."

Because of their widespread distribution, viruses and malware are more likely to strike Android systems, making them an easier target for thieves. Several solutions for detecting these assaults have been proposed, with machine learning being one of the most famous. This is due to the fact that machine learning algorithms may produce a classifier from a complicated set of cases. Spyware detectors may be able to avoid writing extra code by using examples rather than explicitly declaring signatures. Coming up with signature definitions for all conceivable attack circumstances is a complex and time-consuming task, and while there may be no clear rules (signatures) for some of them, examples may be identified quite easily, which is the primary principle in machine learning [3].

Android's internal security has considerably improved since the first Android devices were released with Android 1.6 Donut. Since the launch of Google Play Protect, application privileges have been significantly lowered because they must now request all permissions directly from the user. Security has also been moved to a distinct, upgradable component that is not vendor-specific [4].

The ability to install software (apps) from untrusted sites, on the other hand, is a security flaw in newer Android versions. For hackers, this is a veritable "window of opportunity." As a result, a number of third-party systems for Android app distribution have

Correspondence to: Lisa Angelina, Department of Computer Science, Heidelberg University, Baden-Württemberg, Germany, E-mail: lisaangelina@edu.de

Received: 18-Nov-2022, Manuscript No. JITSE-22-20838; **Editor assigned:** 21-Nov-2022, Pre QC No. JITSE-22-20838 (PQ); **Reviewed:** 07-Dec-2022, QC No. JITSE-22-20838; **Revised:** 14-Dec-2022, Manuscript No. JITSE-22-20838 (R); **Published:** 21-Dec-2022, DOI: 10.35248/2165-7866.22.12.306.

Citation: Angelina L (2022) Machine Learning for Identifying iOS Malware.J Inform Tech Softw Eng. 12:306.

emerged. The downloads available from these sites range from well-known software clones to different malware types.

However, there are additional threats than the platform. Apps may also be loaded and installed into the system using the client, which functions similarly to the official "Google Play" client. Allowing the installation of these programmes opens up a broad range of possibilities for breaking the privacy of the smartphone [5].

CONCLUSION

This article introduced a unique dataset for detecting malware on Android devices. Initially, an overview of the spyware idea and how it affects Android-based smartphone privacy was offered. Furthermore, a better understanding of the Android OS security framework is provided to better comprehend relevant security concerns to users' privacy. Following that, numerous spyware detection methodologies from prior research were explored in order to identify knowledge gaps and demonstrate the necessity for a benchmarked dataset.

REFERENCES

1. Pushpa SS, Sharma K. Review On Spyware-A Malware Detection Using Datamining. Int J Comput Trends Technol.2018;60(3): 157-160.
2. Panda MS. Self propogating malware with varying signature.
3. Girsang AS. Analyzing Android Users Based on Google Play Store Using K-Prototype Algorithm. Int J Emerg Trends Eng Res. 2020;8:2691-2694.
4. Lu S, Guo D, Ren S, Huang J, Svyatkovskiy A, Blanco A, et al. Codexglue: A machine learning benchmark dataset for code understanding and generation. arXiv preprint arXiv: 2102.04664.2021.
5. Tan YA, Xue Y, Liang C, Zheng J, Zhang Q, Zheng J, et al. A root privilege management scheme with revocable authorization for Android devices. J Netw Comput Appl.2018;107:69-82.