

Accepted Manuscript

DroidDet: effective and robust detection of Android malware using static analysis along with rotation forest model

Hui-Juan Zhu , Zhu-Hong You , Ze-Xuan Zhu , Wei-Lei Shi ,
Xing Chen , Li Cheng

PII: S0925-2312(17)31287-0
DOI: [10.1016/j.neucom.2017.07.030](https://doi.org/10.1016/j.neucom.2017.07.030)
Reference: NEUCOM 18718



To appear in: *Neurocomputing*

Received date: 18 March 2017
Revised date: 27 May 2017
Accepted date: 14 July 2017

Please cite this article as: Hui-Juan Zhu , Zhu-Hong You , Ze-Xuan Zhu , Wei-Lei Shi , Xing Chen , Li Cheng , DroidDet: effective and robust detection of Android malware using static analysis along with rotation forest model, *Neurocomputing* (2017), doi: [10.1016/j.neucom.2017.07.030](https://doi.org/10.1016/j.neucom.2017.07.030)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

DroidDet: effective and robust detection of Android malware using static analysis along with rotation forest model

Hui-Juan Zhu¹, Zhu-Hong You^{2,3,*}, Ze-Xuan Zhu^{4,*}, Wei-Lei Shi², Xing Chen⁵, Li Cheng^{2,3}

¹ School of Information Engineering, Yang Zhou University, Yang Zhou 225000, China;

² The Xinjiang Technical Institute of Physics and Chemistry, Chinese Academy of Sciences, Urumqi 830011, China;

³ Xinjiang Laboratory of Minority Speech and Language Information Processing, Urumqi 830011, China;

⁴ College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China;

⁵ School of Information and Control Engineering, China University of Mining and Technology, Xuzhou, 221116, China

* Correspondence: zhuhongyou@ms.xjb.ac.cn (Z.-H.Y.); Tel.: +86-18160622862

Abstract: The Android platform is becoming increasingly popular and various organizations have developed a variety of applications (App) to cater to market trends. Due to the characteristics of the Android platform, such as supporting the unofficial App stores, open source policy and the great tolerance for App verification, it is inevitable that it faces serious problems of malicious software intrusion. In order to protect the users from the serious damages caused by Android malware, we propose a low-cost and high-efficient method to extract permissions, sensitive APIs, monitoring system events and permission-rate as key features, and employ the ensemble Rotation Forest (RF) to construct a model to detect whether an Android App is malicious or not. Specifically, a dataset containing 2,130 samples is used to verify the performance of the proposed method. The experimental results show that the proposed method achieves an high accuracy of 88.26% with 88.40% sensitivity at the precision of 88.16%. To further evaluate the performance of the proposed model, we also compare it with the state-of-the-art Support Vector Machine (SVM) model under the same experimental conditions, and the comparison results demonstrate that the proposed method improves the accuracy by 3.33% compared to SVM. The experimental results show that the proposed model is extremely promising and could provide a cost-effective alternative for Android malware detection.

Download English Version:

<https://daneshyari.com/en/article/6865357>

Download Persian Version:

<https://daneshyari.com/article/6865357>

[Daneshyari.com](https://daneshyari.com)