ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

A Survey Paper on MONET for Malware Variants Detection and Response System in Android Based Cellphone

Shyam S. Gupta[1],Dr Sanjay Kumar Jain[2]

Research Scholar, Shri JJTU, Jhunjhunu, Rajasthan, India[1]

Ph.D. Guide, Shri JJTU, Jhunjhunu, Rajasthan, India[2]

ABSTRACT: Cellphone devices, such as smartphones, have become an important part of modern life. However, as these devices have tremendously become popular they are attracting a range of attacks. Malware is one of the serious threats posed to smartphones by the attackers. Due to the limited resources of cellphone devices malware detection on these devices remains a challenge. Malware detection techniques based on energy-consumption anomaly present several advantages to circumvent the resource constraints of cellphone devices. Here first analysis, runtime behaviours of malware's core functionalities are in fact similar within a malware family. The design and implementation of MONET which has a client and a backend server module. Our analysis shows that MONET can achieve accuracy in detecting malware variants. This paper examines challenges of malware in android and recent progress made in detection techniques. Analysis on how malware has evolved over the last years for the most popular stage. Analyse behaviours pursued goals infection and distribution strategies and provide numerous examples through case studies of the most relevant specimens. The survey classifies and ventilate efforts made in detecting both malware and other suspicious software.

KEYWORDS: Malware detection, Android, Runtime behaviour, Mobile computing, Energy management.

I. INTRODUCTION

The Android working framework has the greatest market in the year 2016. Which makes it the most widely utilized working framework on the planet. This makes the android clients the greatest target gather for malware designers. Consent-based component assumes an indispensable part in android security which constrain the gets to of outsider android applications to impact assets. Bit of Android malware can rise concession by sending short administration messages by influencing calls to protection to numbers sharing nearby data through Global Positioning System (GPS) lastly gathers exceptionally main part of data without the clients learning. The necessity for Android malware recognition is expanded as a security component in android does not define the limit on the framework asset utilization. This is a basic affectability point for pernicious applications.

Mobile Portable innovation has broadened drastically spherical the world. These day shrewd cell phones are utilized for various intention like individual portable correspondence, information stockpiling, and sight and sound budgetary exchanges and furthermore for the amusement. Android is a well-known versatile working framework the purposes behind being favoured by clients are recorded as Open source programming being bolstered by Google applications being created in the most prominent programming dialect Java being open for the customization. Cell phone uses have brought
new data trade to regular day to day existence. The quantity of versatile malware is development rapidly with unmistakable vindictive exercises, for example, taking client individual information sending protection messages and

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

making calls without the client's affirmation. These noxious exercises are escaped the client and they keep running out of sight. Numerous examinations have created strategies to identify such assaults.

II. OBJECTIVE OF THE STUDY

The present study tries to examine a detailed review Malware Variants Detection and Response System in Android.

III. RELATED WORK

In this section, various techniques of Malware Detection are discussed and analysed.

H. Qian and D. Andresen (2015): The author presenting Extending Mobile Device Battery Life by Offloading Computation Cloud. The requirement for growth performance of mobile device directly conflicts with the want for longer battery life. Offloading measurement to resourceful servers is an effective method to rundown energy consumption and enhance performance for mobile applications. Android provides mechanisms for creating mobile applications but not a congenital scheduling system for determining where code should be executed. This paper presents Jade system that adds sophisticated energy aware measurement offloading capabilities to android applications. Jade monitors device and application status and automatically decides where code should be executed. Jade dynamically adjust offloading strategy by adapting to workload variation, communication costs and device status.

K. Xu, Y. Li, and R. H. Deng. (2016): Most existing mobile malware detection methods are designed based on the resources required by malwares (e.g. permissions, application programming interface (API) calls and system calls). These techniques capture the interactions during mobile apps and Android system but ignore the communications among components within application boundaries. As a consequence the majority of the existing techniques are small effective in identifying many typical malwares which need a little or no suspicious resources but leverage on inter component communication (ICC) mechanism. To address this challenge we propose a new malware detection method named ICCDetector. After manually analysing false positives we discover 43 new malwares from the benign data set and rundown the number of false positives to seven. More importantly ICCDetector discovers 1708 more advanced malwares than the benchmark while it misses 220 obvious malwares which can be easily detected by the benchmark.

M. Lindorfer, M. Neugschwandtner, and C. Platzer, Marvin. (2015): In contravention the considerable number of proposed malware analysis systems generic and practical malware analysis solutions are rare and often short-lived. Systems relying on static analysis oneself conflict with growth popular disturbance and dynamic code loading techniques while purely dynamic analysis systems are prone to analysis evasion,he present MARVIN a system that bunch static with dynamic analysis and which transfer machine learning techniques to assess the risk associated with unknown android apps in the form of a hatred score. MARVIN performs static and dynamic analysis both of device to represent properties and behavioural aspects of an app through a rich and comprehensive feature set. In their valuation on the largest android malware distribution data set to date comprised of over 135,000 Android apps and 15,000 malware samples MARVIN correctly classifies 98.24% of malicious apps with less than 0.04% false positives.

H. Qian and D. Andresen. (2015): Android supply mechanisms for creating mobile applications but deficiency a native scheduling system for determining where code should be executed. Jade a system that adds sophisticated energy aware measurement offloading capabilities to android applications. Jade monitors device and application status and automatically determine where code should be executed. Jade dynamically adjusts offloading strategy by adapting to workload difference communication costs and device status. Jade minimizes the burden on developers to construct applications with computation offloading ability by providing easy to use Jade API. Valuation shows that Jade can effectively reduce up to 35% of average power consumption for mobile device while improving application performance.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

W. Enck, D. Octeau, P. McDaniel, and S. Chaudhary. (2011): The fluidity of application markets complex smart-phone security. Although current efforts have light on particular security issues there remains small insight into large security characteristics of smart-phone applications. They introduce the deddecom-piler which retrieval android application source code directly from its installation image. They design and execute a horizontal study of smart-phone applications based on static analysis of 21 million lines of retrieval code. Their analysis uncovered generic use or misuse of personal phone identifiers and deep penetrate of advertising and analytics networks. However we did not find proof of malware or exploitable vulnerabilities in the studied applications. Theywere concluded by considering the implications of these preliminary findings and offer directions for future analysis.

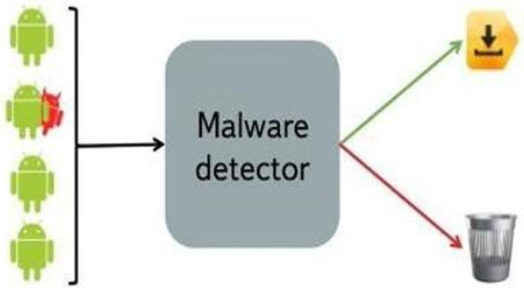

Figure 1: Malware Detector System

According to ZakiraInayat et al in 2016, explain and analysis:

The 5 most imperative parameters needed for IRS, in particular, versatile nature, cost delicate, semantic coherence, oversee false alert, and reaction measurements strategy:

(1) A versatile nature demonstrates that the IRS picks ideal reactions powerfully as indicated by the past reaction achievement and come up failure in upsetting past observed assaults;

(2) IRS is needed to be cost-touchy and have strength for calculating hazard, time and cost, reaction;

(3) Semantic cognizance highlights permit IRS for comprehending the interruption notification and occasions with various sentence structures and semantics (meaningful) from various IDSs;

(4) False caution ratio shows IDS's attribute precision and confidence. Reaction completely depend on the accomplishment of reaction ran in previous and confidence of false caution. None of the present model of architecture s are free of false alarms the reason is that these model of architecture s create false cautions

(5) Similar investigation of IRS demonstrates which current IRS utilizes a static method reaction measurements, reaction choices are constantly in respect of some specific static measurements. The methods studied above are compared in terms of advantages, disadvantages, techniques and accuracy performance. Table 1 is showing the comparative study among these methods.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

Table 1: Malware Detection Techniques			
Paper Title	**Key Techniques and Methods**	**Advantages**	**Disadvantages**
Extending Mobile Device Battery Life by Offloading Computation Cloud.	Offloading Computation Cloud.	Reduce energy consumption and enhance performance for mobile Applications.	Shorten the response time
Mobile Malware Detection	Mobile Malware Detection Methods	Capture the Interactions Between mobile apps and Android system.	Ignore the communications among Components within or cross application boundaries.
Analysis of Malware Detection	Static Analysis Techniques	It is cheap fast not very Resource consuming technique	Have to know Malware patterns Or Signatures in patterns
Analysis of Malware Detection	Dynamic Analysis Techniques	Detection of unknown Attacks	Highly resource consuming not Feasible for Battery Devices
Intelligent Multi-agent system based on Jade	Jade System	Jade can effectively reduce energy consumption of mobile devices, and dynamically change its offloading strategy according to device status.	Decrease Low performance because of code offloading.

Later on research the fresh techniques and comparing their performances. In this portion the going drawbacks and research challenges are noted for future work. Working on EEMONET is very imperative now days hence its must that technique should be capability of all malware detection in all viewpoint. Recently many researchers did work to deliver the best solution to Detect Malware in Android but we had below observations through our study.

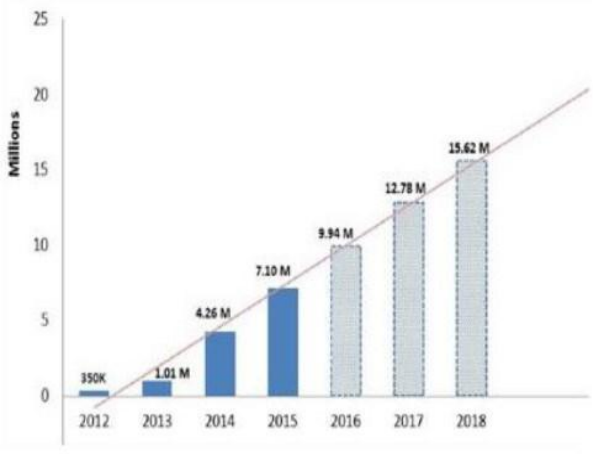

Figure 2: Future Trends of Android Malware Growth

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

Two approaches of malware detection from users mobile such as static malware detection and dynamic intrusion detection systems. In literature under these two categories number of solutions introduced but suffered from the limitations in terms of efficiency and scalability. Such methods are not supporting to scan the runtime behaviors of malware in order to detect them successfully. Recently another hybrid solution introduced in which runtime behavior with static structures is combined to detect malware variants efficiently this method called as Monet. The problem identified with Monet is power consumption or energy efficiency is not addressed while malware detection. This require study towards effectively and efficiently energy save by considering anomaly based intrusion/malware detection as well as for its prevention for smart phone.

IV. CONCLUSION

The malware are ordered based on location techniques they utilize. An itemized execution assessment of these malware procedures is likewise supply and the points of interest and the advantages and limitations of these malware are deduced comprehensively. Idea of hybrid malware is introduced which will address the impediments of existing static and dynamic methodologies. In future it is expected to execute the proposed hybrid solution which will be a nonspecific malware that will give better security to android gadgets by right off the bat statically breaking down the Android applications on nearby gadget and afterward it will perform dynamic investigation on a remote malware server. This will expend little measure of memory space on the gadget and the battery utilization will likewise be low as all powerful investigation will be performed at the remote server.

REFERENCES

[1] D. Arp, M. Spreitzenbarth, M. H ubner, H. Gascon, K. Rieck, and C. Siemens, Drebin: Effective and explainable detection of android malware in your pocket, in Prof. of the Network and Distributed System Security Symposium, 2014.

[2] F. Wei, S. Roy and S. Ou. Amandroid: A Precise and General Intercomponent Data Flow Analysis Framework for Security Vetting of Android Apps. In proceedings of the 2014 ACM Conference on Computer and Communications Security. 2014.

[3] H. Qian and D. Andresen. An Energy-saving Task Scheduler for Mobile Devices. In Proceedings of the 14th IEEE/ACIS International Conference onComputerandInformationScience (ICIS), 2015.

[4] H. Qian and D. Andresen. Emerald: Enhance Scientific Workflow Performance with Computation Offloading to the Cloud. In Proceedings of the 14th IEEE/ACIS International Conference on Computer and Information Science (ICIS), 2015.

[5] H. Qian and D. Andresen. Extending Mobile Devices Battery Life by Offloading Computation to Cloud. In Proceedings of the 2nd ACM [1] International Conference on Mobile Software Engineering and Systems (MOBILESoft), 2015.

[6] K. Xu, Y. Li, and R. H. Deng, Iccdetector: Icc-based malware detection on android, TIFS, 2016.

[7] L. Peng, Y. Yang et al. Highly Accurate Video Object Identification Utilizing int Information. In proceedings of the International Conference on Computing, Networking and Communications (ICNC), 2014.

[8] Q. Chen, H. Qian et al. BAVC: Classifying Benign Atomicity Violations via Machine Learning. In Advanced Materials Research, Vols 765-767, pp. 1576-1580, Sep, 2013.

[9] S. Roy, J. DeLoach, Y. Li, N. Herndon, D. Caragea, X. Ou, V. P.Ranganath, H. Li, and N. Guevara, Experimental study with realworld data for android apps security analysis using machine learning, in ACSAC. ACM, 2015.

[10] S. Zhang, X. Zhang and X. Ou. After We Knew It: Empirical Study and Modeling of Cost-effectiveness of Exploiting Prevalent Known Vulnerabilities Across IaaS Cloud. In proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2014.

[11] ZakiraInayat et al., 2016 "Intrusion response systems: Foundations, design, and challenges". JNCA 62, pp 53–74.