Abstract

With the rapid arrival of mobile platforms on the market, android Platform has become a market leader in 2015 Q2, according to IDC. As Android has ruling most of the market, the problem of malware threats and security is also increasing. In this review paper, a fastidious study of the terms related to mobile malware and the techniques used for the detection of malware is done. Some proposed methods and type of approaches used in those methods are also summarized.

References


5. Huang, C.Y., Tsai, Y.T. and Hsu, C.H. 2013. Performance evaluation on
permission-based detection for android malware, Advances in Intelligent Systems and

by applying machine learning classifiers on static features: A state-of-art survey, Journal of


8. Schmidt, A.D. 2009. Static analysis of executables for collaborative malware detection on


android application sandbox system for suspicious software detection, 5th International

versatile protection for smartphones, Proc. of the 26th Annual Computer Security Applications

using the knowledge-based, temporal abstraction method, Journal of Systems and Software,

behavioural malware detection framework for android devices, Journal of Intelligent Information

15. Enck, William, Gilbert, P., Han, S., Tendulkar, V., Chun, B.G., Cox, L. P., Jung, J.,
McDaniel, P. and Sheth, A.N. 2014 TaintDroid: An information-flow tracking system for realtime
privacy monitoring on smartphones, Journal of ACM Transactions on Computer Systems
(TOCS), vol. 32, 2014, article 5.

281-294.

iOS applications, In NDSS, 18th Annual Network and Distributed System Security Symposium,
San Diego, CA, USA, 2011.

detection system for android, Proceedings of the 1st ACM workshop on Security and privacy in

Index Terms

Computer Science Information Sciences

Keywords

Malware, Types of malware, Detection techniques, Permissions.