





















- [3] X. Ju, "Android malware detection through permission and package," In *2014 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR)*, 61-65, 2014.
- [4] C. Tansettanakorn, S. Thongprasit, S. Thamkongka, and V. Visoottiviseth, "ABIS: a prototype of android botnet identification system, In *Student Project Conference (ICT-ISPC)*, 1-5, 2016.
- [5] M. Yusof, M. Mohd Saudi, and F. Ridzuan, "A New Android Botnet Classification for GPS Exploitation Based on Permission and API Calls," In *International Conference on Advanced Engineering Theory and Applications*, Springer, Cham, 27-37, 2017.
- [6] N. Maryam, S. Soltani, and S. A. Seno, "Android malware detection based on overlapping of static features," In *7th International Conference on Computer and Knowledge Engineering (ICCKE 2017)*, Ferdowsi University of Mashhad, Oct. 26-27, 2017.
- [7] P. Wonjoo, K. Lee, K. Cho, and W. Ryu, "Analyzing and detecting method of android malware via disassembling and visualization, " In *Information and Communication Technology Convergence (ICTC), 2014 IEEE International Conference*, 817-818, 2014.
- [8] J. Xuxian, and Y. Zhou, "Dissecting android malware: Characterization and evolution," In *2012 IEEE Symposium on Security and Privacy*, 95-109, 2012.
- [9] C. Jian, H. Manar, R. Thomas, and Y. Zou, "Detecting android malware using clone detection," *Journal of Computer Science and Technology*, vol. 30, no. 5, pp. 942-956, 2015.
- [10] W. Zhaoguo, C. Li, Y. Guan, Y. Xue, and Y. Dong, "ActivityHijacker: Hijacking the Android Activity Component for Sensitive Data," In *Computer Communication and Networks (ICCCN), 25th IEEE International Conference*, 1-9, 2016.
- [11] H. Shun-Wen, S. Yeali and M. C. Chen, "Behavior grouping of Android malware family." In *ICC*, pp. 1-6. 2016.
- [12] Y. Chunyong, and S. Zhang, "Parallel implementing improved k-means applied for image retrieval and anomaly detection," *Journal of Multimedia Tools and Applications*, vol. 76, no. 16, pp. 16911-16927, 2017.
- [13] G. Fei, J. Niu, Z. Qi, and M. Atiquzzaman, "Partitioning and offloading in smart mobile devices for mobile cloud computing: State of the art and future directions," *Journal of Network and Computer Applications*, vol. 3, no. 2, pp. 42-56, 2018.
- [14] W. Markus, F. Fischer, R. Luh, A. Haberson, A. Rind, and A. Keim, "A survey of visualization systems for malware analysis," In *EG Conference on Visualization (EuroVis)-STARs*, 105-125, 2015.
- [15] Linux Malware Detect - Rfx Networks, 2017. [Online] Available: <https://www.rfxn.com/projects/linux-malware-detect/>.
- [16] Engauge Digitizer [Online]. Available <http://markumitchell.github.io/engauge-digitizer/>
- [17] Asaf, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, "Anomaly: a behavioural malware detection framework for android devices," *Journal of Intelligent Information Systems* vol. 38, no.7, pp. 161-190, 2012.
- [18] Method and Processes for Securely Autofilling Data Fields in A Software Application, by Caron, Etienne. (2018, January 4). U.S. Patent Application 15/707,647.
- [19] J. Hao, H. Yang, S. Qin, Z. Su, J. Zhang, and J. Yan, "Detecting Energy Bugs in Android Apps Using Static Analysis," In *International Conference on Formal Engineering Methods*, Springer, Cham, 192-208, 2017.
- [20] W. Andrew, P. K. Ferentinos, and P. G. Petropoulos, "A new synergistic approach for monitoring wetlands using Sentinels-1 and 2 data with object-based machine learning algorithms," *Journal of Environmental Modelling & Software*, vol. 6, no 104, pp. 40-54, 2018.