How to avoid downloading malware on a personal device

In the generation of technology, there are many threats along with the new invention of many gadgets. Almost every person in the world uses smart-phones and other personal devices. There are many softwares created everyday for these devices and are installed by people. Our technology has improved so much that we are dependent upon softwares for our daily works. There are many sites and browsers where we can download applications for our daily lives. Smart phones have become popular companions in people’s daily life which allow users to access news, entertainment, carryout research or make purchases via e-businesses. Most of the malware are web based these days which became a threat in today’s Internet Security. The example of android malware behavior can be taken malware visualization and its platform can be studied. To learn about the malware behaviour in android we can use “four components: the Embedded client and the Sink on the smartphone side, and the Web Service and the Visualization component on the remote server side.”(Somarriba,2016).

Android malware can be a good example for the analysis of malware in a personal device. Over six million mobile malware samples have been accumulated by McAfee as of Q4 2014, up 14% over Q3, and roughly 98% of them target primarily Android devices [McAfee 2015].(TAM, K., FEIZOLLAH, A., ANUAR, N. B., SALLEH, R., & CAVALLARO, L. (2017)). These malwares became the greatest threats to the users personal, sensitive and enterprise information to hackers. Because of this the attackers are earning a lot of money and causing loss to the victims in every way. The focus on the leakage of Android Apps is increasing due to the continuous increase of Android system market share. In 2010, the first SMS (Short Message Service) Trojan in Android system was released by Kaspersky and was used to steal personal property of users.(Zhou, Q., Feng, F., Shen, Z., Zhou, R., Hsieh, M., & Li, K. (2018)).

There are “three categories of defense mechanisms are discussed in detail: (1) building honeypots with virtual machines or signature-based detection system to discover existing threats; (2) using code analysis and testing techniques to identify the vulnerabilities of Web applications; and (3) constructing reputation-based blacklists or smart sandbox systems to protect end-users from attacks.”(Chang,2013).

References

Somarriba, O., Zurutuza, U., Uribeetxeberria, R., Delosières, L., & Nadjm-Tehrani, S. (2016). Detection and Visualization of Android Malware Behavior. Journal of Electrical & Computer Engineering, 1–17. https://doi-org.ez.lib.jjay.cuny.edu/10.1155/2016/8034967

JIAN CHANG, VENKATASUBRAMANIAN, K. K., WEST, A. G., & INSUP LEE. (2013). Analyzing and Defending Against Web-Based Malware. ACM Computing Surveys, 45(4), 49–49:35.<https://doi-org.ez.lib.jjay.cuny.edu/10.1145/2501654.2501663>

Juan Alegre-Sanahuja, Javier Camacho, Juan Carlos Cortés López, Francisco-José Santonja, & Rafael Jacinto Villanueva Micó. (2014). Agent-Based Model to Study and Quantify the Evolution Dynamics of Android Malware Infection. Abstract and Applied Analysis, 2014, 1–10.<https://doi.org/10.1155/2014/623436>

TAM, K., FEIZOLLAH, A., ANUAR, N. B., SALLEH, R., & CAVALLARO, L. (2017). The Evolution of Android Malware and Android Analysis Techniques. ACM Computing Surveys, 49(4), 76:1-76:41. <https://doi-org.ez.lib.jjay.cuny.edu/10.1145/3017427>

Zhou, Q., Feng, F., Shen, Z., Zhou, R., Hsieh, M., & Li, K. (2018). A novel approach for mobile malware classification and detection in Android systems. Multimedia Tools and Applications, 78(3), 3529–3552. https://doi.org/10.1007/s11042-018-6498-z