A Cloud-Based Anti-Malware Solution

In this work we focus on cloud-based malware detection. We investigate the existing academic and industry solutions to detect malware on top of cloud services, and the drawbacks of those solutions. We also provide a remediation for the drawbacks of those solutions. At the end we provide an overview of our proposed cloud-based anti-malware approach. We study two main industry solutions, namely, Trend Micro, and Panda Security. While Trend Micro provides commercial products, Panda Security provides free anti-virus product. Both of them adapted cloud computing to their malware detection solution in different ways. Trend Micro provides distinct products for distinct services (i.e., Messaging Security to detect potential spam, and OfficeScan & Smart Detection Network product to detect threats at the end-user machines), while Panda security provides one product to correlate all possible threats and exploits information together and provide protection to all kinds of attacks. We chose to cover these two corporation solutions in detail. However, there is a lack of information on their fundamental techniques due to the fact that they are unaddressed in their whitepapers because they are profit making companies. Moreover we made an objective comparison between both solutions, in terms of their impact at the end-user front-end, network front- end, and improvement of malware protection. Similarly we explored all new academic research on cloud-based malware detection available in the public domain. We found that three of them are the most relevant to cloud-based malware detection. Although the basic idea, motivation and objective of each one of them are distinct; they all include some merits that can foster ongoing research in this area. We compared between these solutions carefully, including their benefits and drawbacks. Also, we took some liberty in interpreting those solutions with respect to their objectives and techniques, this helps us to find some commonality between them and the earlier discussed industry solutions. People in industry tend to avoid mentioning these relationships in order to protect their copyrights and hide the drawbacks of their solutions. We have presented a comprehensive paper on cloud-based anti-malware detection problems and solutions including both industry and academic views, and we learnt from our research results to develop a new solution that preserve end-users data privacy and minimize the resulting overhead in their machines. This solution supports different granularity of protection levels, and also adapt different user preferences. Furthermore, it can facilitate both forensic tracing and retrospective detection without compromising end-users privacy. At the end of this work we made some suggestions and guidelines for researchers who are interested in this area, these guidelines recommend the good practices that should be followed in any solution, and the minimum requirements & constraints that should be met.

Primary authors : Prof. JENG, Albert (Jinwen University of Science and Technology) ; Mr. AL-TAHARWA, Ismail Adel (Dept. of CSIE, NTUST)

Co-authors : Prof. LEE, Hahn-ming (Dept. of CSIE, NTUST) ; Prof. CHEN, Shyi-ming (Dept. of CSIE, NTUST)