Improvements for Behavior Based Malware Detection Solutions

Mondoc Alexandra

Faculty of Computer Science, Babeş-Bolyai University, Cluj-Napoca, Romania

alexandra@cs.ubbcluj.ro

The number of malicious applications is growing almost exponentially. In addition, the increased complexity and sophistication of malicious software represents a serious threat to users. To combat these threats, advanced security solutions, such as dynamic behavior based solutions, have been developed. As the effectiveness of this layer of protection is increasingly recognized, potential beneficiaries continue to be concerned about the ways their day-by-day activity might be affected by the performance overhead produced by a security solution. Such overhead is especially noticeable in behavior based solutions, because they need to monitor and analyze the actions performed by processes on a system. We propose a solution for this issue and attempt to alleviate the system slowdown produced by dynamic behavioral security solutions.

References

[1] Hăjmăşan, G., Mondoc, A., Creţ, O.: Dynamic behavior evaluation for malware detection. In: 2017 5th International Symposium on Digital Forensic and Security (ISDFS). pp. 1–6 (April 2017)

[2] Ji, Y., Li, Q., He, Y., Guo, D.: Overhead analysis and evaluation of approaches to host-based bot detection. International Journal of Distributed Sensor Networks 11(5), 524627 (2015)

[3] Mircescu, D.: Systems and methods for using a reputation indicator to facilitate malware scanning (august 2015), US Patent 9,117,077

[4] Uluski, D., Moffie, M., Kaeli, D.: Characterizing antivirus workload execution 33, 90–98 (03 2005)

[5] Vasiliadis, G., Ioannidis, S.: GrAVity: A Massively Parallel Antivirus Engine, pp. 79–96. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)