IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

Malware Detection Using Machine Learning Algorithms

Dr. Vajid Khan[1], Shriyansh Dubey[2], Sandeep Yadav[3], Vishal Gaikwad [4], Nishit Jambhulkar[5]
Professor, Computer Engineering, DPCOE, Pune, India[1]
Student, Computer Engineering, DPCOE, Pune, India[2,3,4,5]

Abstract: *In the present world, current antivirus software is only effective against known viruses if the malware contains new viruses, with signatures in place, it's hard to tell if it's malicious. Signature-based detection is less effective against zero-day attacks. Until the new hidden malware is detected it may spread in your computer system. This malware can exploit your system. According to research, malware has been found in the last 10 years it grew exponentially and caused significant economic losses to various organizations. Various antivirus companies are proposing solutions to protect against this malware attack. With the increasing speed, quantity, and complexity of viruses, malware poses new challenges to the antivirus community. The current state of research shows that researchers and antivirus organizations have recently begun to apply machine learning and deep learning techniques to analyse and detect various malwares. You can use machine learning techniques to create more effective antivirus software that can detect previously unknown and known malware, zero-day attacks, and more. In our project, we have proposed an approach that uses various machine learning methods and algorithms such as Vector Machine (SVM), Random Forest, and XGBoost.*

Keywords: Malware detection, virus, data mining, Information gain, random forest, machine learning, classification, enterprise, network, security.

REFERENCES

[1] http://www.us-cert.gov/control_systems/pdf/undirected_attack0905.pdf
[2] "Defining Malware: FAQ". http://technet.microsoft.com. Retrieved 2009-09-10.
[3] F-Secure Corporation (December 4, 2007). "F-Secure Reports Amount of Malware Grew by 100% during 2007". Press release. Retrieved 2007-12-11.
[4] History of Viruses. http://csrc.nist.gov/publications/nistir/threats/subsubsection3_3_1_1.html
[5] Landesman, Mary (2009). "What is a Virus Signature?" Retrieved 2009-06-18.
[6] Christodorescu,M., Jha, S., 2003. Static analysis of executables to detect malicious patterns. In: Proceedings of the 12th USENIX Security Symposium. Washington.pp. 105-120.
[7] Filiol, E.,2005. Computer Viruses: from Theory to Applications. New York, Springer, ISBN 10: 2287-23939-1.
[8] Filiol, E., Jacob, G., Liard, M.L., 2007: Evaluation methodology and theoretical model for antiviral behavioral detection strategies. J. Comput. 3, pp 27–37.
[9] H. Witten and E. Frank. 2005. Data mining: Practical machine learning tools with Java implementations. Morgan Kaufmann, ISBN-10: 0120884070.
[10] J. Kolter and M. Maloof, 2004. Learning to detect malicious executables in the wild. In Proceedings of KDD'04, pp 470-478.
[11] J. Wang, P. Deng, Y. Fan, L. Jaw, and Y. Liu, 2003.Virus detection using data mining techniques. In Proceedings of IEEE International Conference on Data Mining.
[12] Kephart, J., Arnold, W., 1994. Automatic extraction of computer virus signatures. In: Proceedings of 4th Virus Bulletin International Conference, pp. 178–184.