IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, May 2022
Impact Factor: 6.252

Malware Detection Using Machine Learning

Shreya Mohanki[1], Shreya Shinde[2], Preeti Pisal[3], Manasi Manikumar[4], Prof. Sagar Dhanake[5]
Students, Department of Computer Engineering[1,2,3,4]
Assistant Professor, Department of Computer Engineering[5]
Dr. D. Y. Patil Institute of Technology, Pune, Maharashtra, India

Abstract: *Malware detection is the study and prevention of malicious software in the realm of computer security. It isn't the only way to protect a business against a cyber-attack. Companies as well as administrators must assess their risk in order to be effective. In this study, we will look at many different ways of detecting computer malware and malicious software, websites, as well as future instructions in this field of study, and we'll also talk about the rise of computer viruses and worms and how to combat them. Innovative procedures and strategies such as the behavioral-based model and the signature-based model are replacing traditional detection methods. Future instructions will include the development of improved security solutions to combat cyber fraud, which has increased in recent years, particularly in the Asia-Pacific region. With the rise in cyber security fraud and other dangerous activities, traditional approaches are no longer sufficient to protect computers, as they have numerous limitations. To address these challenges, researchers have developed new techniques such as heuristic analysis and static and dynamic analysis, which can detect over 90% of malware samples with no false positives or negatives.*

Keywords: Behaviour-based approach, Dynamic analysis, Static analysis, Heuristic, Malware, Ransomware, Signature-based model, Vulnerability

REFERENCES

[1]. W. Han, J. Xue, Y. Wang, L. Huang, Z. Kong, Mal DAE : Detecting and explaining malware based on correlation and fusion of static and dynamic characteristics, Computer Secure 83 (2019) 208–233, http://dx.doi.org/10.1016/j.cose.2019.02. 007.

[2]. P. Burnap, R. French, F. Turner, K. Jones, Malware classification using self organising feature maps and machine activity data, Computer Secure 73 (2017) 399–410, http://dx.doi.org/10.1016/j.cose.2017.11.016, http://linkinghub.elsevier.com/retrieve/pii/S0167404817302535.

[3]. A. Damodaran, F.D. Troia, C.A. Visaggio, T.H. Austin, M. Stamp, A comparison of static, dynamic, and hybrid analysis for malware detection, J. Comput. Virol. Hacking Tech. 13 (1) (2017) 1–24, http://dx.doi.org/10.1007/s11416- 015-0261-z.

[4]. E.M. Dovom, A. Azmoodeh, A. Dehghantanha, D.E. Newton, R.M. Parizi, H. Karimipour, Fuzzy pattern tree for edge malware detection and categorization in iot, J. Syst. Archit. 97 (March) (2019) 1–7, http://dx.doi.org/10.1016/j.sysarc. 2019.01.017.

[5]. M. Ficco, F. Palmieri, Leaf : An open-source cyber security training platform for realistic edge-iot scenarios, J. Syst. Archit. 97 (September 2018) (2019) 107–129, http://dx.doi.org/10.1016/j.sysarc.2019.04.004.