RESEARCH ARTICLE | SEPTEMBER 05 2023

Malicious software detection using ML algorithms

Sohith Tummala ; Prithvi Sriman Maddukuri;
Niranjana Nitish Varma Bhupathiraju; Mallikarjuna Rao Cherukupalli;
Srujan Singam

+ Author & Article Information

AIP Conf. Proc. 2754, 020007 (2023)

https://doi.org/10.1063/5.0161055

Malicious software is designed to cause devastation on computer systems. Dynamic and static analysis techniques are widely used to examine malware. Unique patterns are categorised and predicted using such approaches, allowing malware to be detected appropriately. Many malware detection strategies have been proposed in the last decade utilising different techniques. Distributed Denial of Service Cyber Attacks are quite familiar security problems, with the majority of them being network-based. They usually include overburdened network devices that request more than what they can manage, which limits the server from responding to the valid requests. Software presents an extremely high security risk. Software assaults have a potential to corrupt or destroy devices, and compromise whole systems, abscond data, change data, block access, and harm or damage data. We are particularly interested in employing machine learning techniques in order to construct a malware detection system utilising dynamic analysis. Our study presents a behaviour-based malware detection method. We built an environment for dynamic analysis as well as used classification algorithms to run malware samples to create this method. Then, for malware detection systems, several behaviour artefacts such as Application Program Interface calls, Printable String Information, check list changes, file actions, and so forth were extracted. We built an environment for dynamic analysis as well as used classification algorithms to run malware samples to build

Information technology, **Computer systems**, **Machine learning**, **Application programming interface**

REFERENCES

1. M. Alaeiyan, S. Parsa, M. Conti, *Computer Communications* 136, 76–90(2019).
https://doi.org/10.1016/j.comcom.2019.01.003
Google Scholar Crossref

2. S.M. Bidoki, S. Jalili, A. Tajoddin, *Engineering Applications of Artificial Intelligent* 60, 57–70(2017).
https://doi.org/10.1016/j.engappai.2016.12.008
Google Scholar Crossref

3. Y. Ki, E. Kim, H.K. Kim, *International Journal of Distributed Sensor Networks* 6,1–9(2015).
Google Scholar

4. Z. Pan, C. Feng, C. Tang, (2016). “Malware classification based on the behavior analysis and back propagation neural network,” in *ITM Web of Conferences* (ITA, 2016),pp. 1–5.
Google Scholar

5. I.K. Cho, T.G. Kim, Y.J. Shim, M. Ryu, E.G. Im, *Intelligent Automation and soft computing* 22, 371–377(2016).
https://doi.org/10.1080/10798587.2015.1118916
Google Scholar Crossref

6. B. N. Narayanan, O. Djaneye-Boundjou and T. M. Kebede, "Performance analysis of machine learning and pattern recognition algorithms for Malware classification," 2016 IEEE National Aerospace and Electronics Conference (NAECON) and Ohio Innovation Summit (OIS), (IEEE, Dayton, OH, USA, 2016), pp. 338–342.
Google Scholar Crossref

7. F. Mira, A. Brown and W. Huang, "Novel malware detection methods by using LCS and LCSS," in 22nd International Conference on Automation and Computing (ICAC), (IEEE, Colchester, UK, 2016), pp. 554–559.
Google Scholar Crossref

8. R. S. Pirscoveanu, S. S. Hansen, T. M. T. Larsen, M. Stevanovic, J. M. Pedersen and A. Czech, "Analysis of

Malware behavior: Type classification using machine learning," in *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, (IEEE, London, UK, 2015), pp. 1–7
Google Scholar

9. W. Mao, Z. Cai, D. Towsley, Q. Feng, X. Guan, *Comp. Secur.* 68, 47–68 (2017).
https://doi.org/10.1016/j.cose.2017.02.009
Google Scholar Crossref

10. A. Pektaş, T. Acarman, *Journal of. Information Security and Applcation* 37, 91–100(2017).
https://doi.org/10.1016/j.jisa.2017.10.005
Google Scholar Crossref

11. S. Huda, R. Islam, J. Abawajy, J. Yearwood, *Future Generation Computer Systems* 83, 193–207(2018).
https://doi.org/10.1016/j.future.2017.12.037
Google Scholar Crossref

12. Q. Le, O. Boydell, B. Mac, M. Scanlon, *Digit. Invest.*26, S118–S126(2018). https://doi.org/10.1016/j.diin.2018.04.024
Google Scholar Crossref

Register Reset password

Pay-Per-View Access
$40.00

BUY THIS ARTICLE