IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

Malware Detection and Analysis Using YARA Tool

Bhargavi Jadhav[1] and Malhar Jadhav[2]
Department of Computer Engineering
Cummins College of Engineering, Mumbai, India[1]
HDFC, Mumbai, India[2]

Abstract: *Malicious software, or malware, is one of the biggest threats to the vast amounts of data and files handled today. One widely used tool for malware detection is YARA(Yet Another Recursive Acronym), which uses YARArules to match suspicious content in files or network packets analyzed by antivirus engines. It works with most hosts running Windows, Linux, or Mac operating systems. However, while YARA is effective, its scanning process can be quite slow, especially with large datasets. This paper explores ways to optimize YARA's scanning process to make it faster and more efficient. We discuss various modes available within YARA to enhance performance, such as fast mode for quicker scanning and recursive mode for in-depth analysis. By fine-tuning these settings, we aim to reduce scan times without compromising detection accuracy.*

Keywords: YARA tool, Malware Detection, Yara Modes, Pattern Matching