

EFFECTIVELY WRITING YARA RULES TO DETECT MALWARES

A PROJECT REPORT

Submitted by,

Ms. Meenakumari B M	-	20211CSG0032
Ms. Harshitha M	-	20211CSG0014
Mr. Suhaas R	-	20211CSG0019
Ms. Supritha G M	-	20221LCG0006

Under the guidance of,

Ms. Riya Sanjesh

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND TECHNOLOGY

At



PRESIDENCY UNIVERSITY

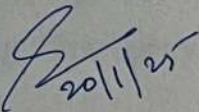
BENGALURU

JANUARY 2025

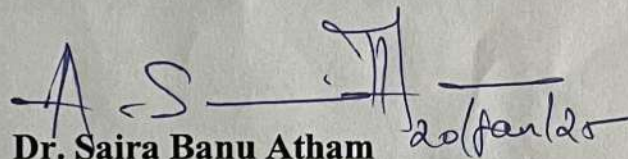
PRESIDENCY UNIVERSITY
PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND
ENGINEERING

CERTIFICATE

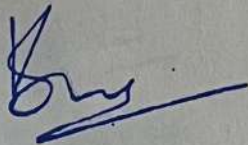
This is to certify that the Project report “Effectively Writing Yara Rules To Detect Malwares” being submitted by “Meenakumari B M, Harshitha M, Suhaas R, Supritha G M” bearing roll number(s) “20211CSG0032, 20211CSG0014, 20211CSG0019, 20221LCG0006” in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Technology is a bonafide work carried out under my supervision.



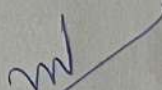
Ms. Riya Sanjesh
Assistant Professor
Presidency School of CSE
Presidency University




Dr. Saira Banu Atham
Professor & HoD
Presidency School of CSE
Presidency University



Dr. L. SHAKKEERA
Associate Dean
Presidency School of
CSE
Presidency University



Dr. MYDHILI NAIR
Associate Dean
Presidency School of
CSE
Presidency University



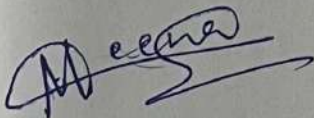
Dr. SAMEERUDDIN KHAN
Pro-Vc Presidency School of
Engineering
Dean - Presidency School of
CSE&IS
Presidency University

PRESIDENCY UNIVERSITY
PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND
ENGINEERING

DECLARATION

We hereby declare that the work, which is being presented in the project report entitled **EFFECTIVELY WRITING YARA RULES TO DETECT MALWARES** in partial fulfillment for the award of Degree of **Bachelor of Technology in Computer Science and Technology**, is a record of our own investigations carried under the guidance of **Ms. Riya Sanjesh**, Assistant Professor, Presidency School of Computer Science Engineering, Presidency University, Bengaluru.

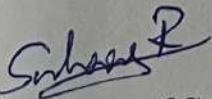
We have not submitted the matter presented in this report anywhere for the award of any other Degree.



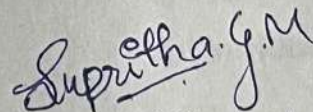
Signature of Student
Name: Meenakumari B M
Roll: 20211CSG0032



Signature of Student
Name: Harshitha M
Roll: 20211CSG0014



Signature of Student
Name: Suhaas R
Roll: 20211CSG0019



Signature of Student
Name: Supritha G M
Roll: 20221LCG0006

ABSTRACT

YARA, an acronym for "Yet Another Recursive Acronym," has become an essential tool in malware detection and analysis due to its ability to classify and identify files based on defined patterns. Developing efficient YARA rules is a challenging endeavor that demands substantial expertise and meticulous attention to detail. Challenges include the need for accurate signatures to minimize false positives and negatives, creating generic rules that cover multiple malware samples, and optimizing scanning performance on large datasets. This project addresses these challenges by proposing a comprehensive framework to automate, refine, and enhance the YARA rule-writing process.

A key focus of this study is creating a search engine to streamline the **selection of YARA signature patterns**. This tool assists analysts in identifying optimal patterns that are both specific to malware behavior and versatile enough to cover related samples. The search engine streamlines the rule-writing process by suggesting highly relevant patterns, thereby reducing the time and effort required for manual signature crafting.

To further enhance the usability of YARA, the project introduces a method for **automatically generating YARA rules** based on a specific set of files. This approach ensures that generated rules effectively capture distinguishing features of the target files while maintaining generality, allowing a single rule to detect multiple malware variants. By focusing on shared characteristics of malware families, this method reduces the need for creating numerous rules for closely related samples.

A significant contribution of this project is the focus on **reducing scanning time** when applying YARA rules to large datasets. Malware analysts often need to evaluate large volumes of clean and malicious files to identify the most effective signature candidates. The proposed system employs optimization techniques to minimize computational overhead, ensuring that the scanning process remains efficient even with extensive datasets. This efficiency is critical for real-world scenarios where timely detection can mitigate threats more effectively.

In summary, this project provides a scalable, efficient, and automated approach to writing YARA rules that address key challenges in malware detection. The contributions include a signature search engine, automated rule generation, and optimization techniques for large-scale scanning. These advancements offer valuable tools for malware analysts and researchers, enhancing their ability to combat evolving cyber threats effectively. This work represents a step forward in malware detection technology, providing a robust solution to challenges in rule-based analysis.