Malware Protection using Reverse Engineering

Department of Computer Science and Engineering
PES University, RR Campus, Bengaluru - 560085.

PROBLEM STATEMENT

- This project aims to establish a robust framework designed to empower individuals with the knowledge and tools necessary to comprehend, detect, and effectively counteract malware threats.

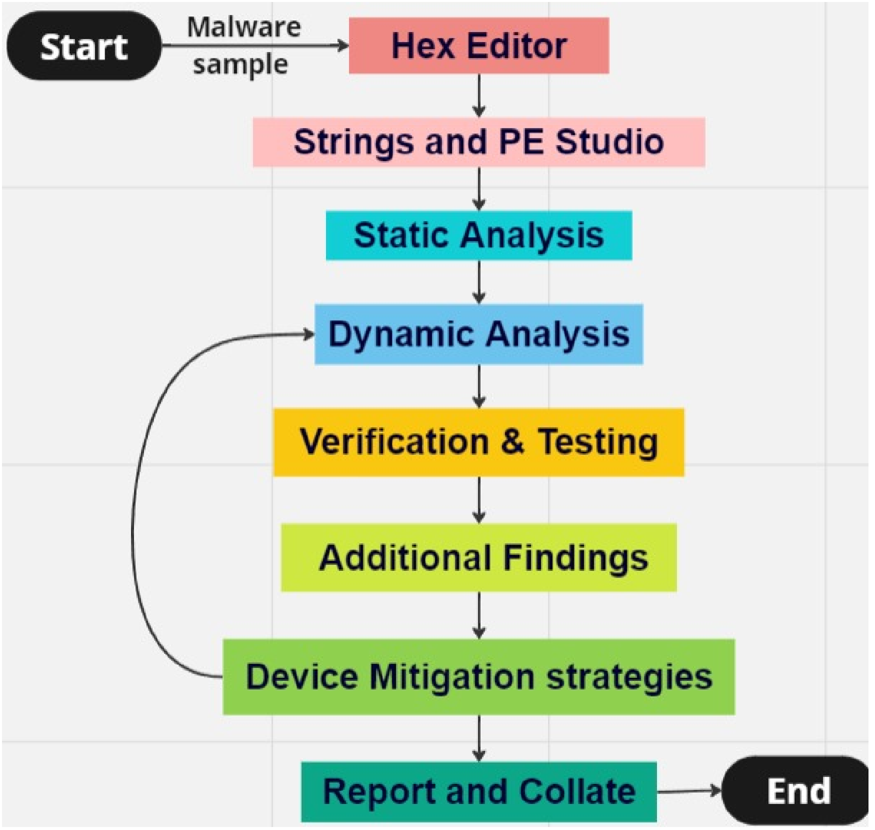
BACKGROUND

- In reverse engineering, the synergy of static and dynamic analysis is key. Ghidra excels in static analysis, offering robust capabilities.
- For dynamic analysis, the Sysinternals suite stands out as a preferred open-source tool.
- Analysing Windows malware is most effective in an isolated environment, such as Flare VM, ensuring a controlled and secure analysis space.

DATASET AND FEATURES / PROJECT REQUIREMENTS/ PRODUCT FEATURES

- Encryption based malware samples like Virlock , Macros like Punjex Dropper, Evasive malware like MalBen Dropper and Information stealers like RedLine stealer are some of the malware samples that we selected/crafted for analysis.

DESIGN APPROACH / METHODS



RESULTS AND DISCUSSION

- The project yielded 16 detailed reports on malware analysis procedures, accompanied by cheat sheets for PowerShell and DLL API calls.
- A comprehensive document outlining the steps for setting up an effective malware analysis environment is also provided. Research papers addressing gaps in analysis augment the project contributions.

SUMMARY OF PROJECT OUTCOME

- The resulting framework encompasses diverse components of malware, offering insights and best practices essential for tackling these threats.
- By adopting a dual perspective—both as an attacker and a defender—this framework provides a comprehensive approach to malware analysis.

CONCLUSION AND FUTURE WORK

- In conclusion, this project's comprehensive framework, developed through the exploration of existing tools and reverse engineering real-world malware samples, stands as a pivotal resource for cybersecurity society.
- For future endeavors, it is imperative to focus on the development of cutting-edge tools aligned with the latest malware trends

REFERENCES

- M. Kim, H. Cho and J. H. Yi, "Large-Scale Analysis on Anti-Analysis Techniques in Real-World Malware," in IEEE Access, vol. 10, pp.
- Fok Kar Wai and Vrizlynn L. L. Thing, ”Clustering based opcode graph generation for malware variant detection”, from 2021 18th International Conference on Privacy, Security and Trust (PST), Dec, 2021, IEEE, https://doi.org/10.1109/pst52912.2021.9647814

Pavan R Kashyap
PES1UG20CS280

Phaneesh Katti
PES1UG20CS281

Hrishikesh Bhat P
PES1UG20CS647

Pranav K Hegde
PES1UG20CS672

Prof. H. B. Prasad
Project Guide

Asst. Prof. Sushma A. E.
Project Co-Guide