

A framework for automated protocol reverse engineering and study of botnet command and control protocols

1st Given Name Surname

dept. name of organization (of Aff.)

name of organization (of Aff.)

City, Country

email address or ORCID

2nd Given Name Surname

dept. name of organization (of Aff.)

name of organization (of Aff.)

City, Country

email address or ORCID

Abstract—TODO redact this at the end

Index Terms—TODO keywords

REFERENCES

- [1] G. Eason, B. Noble, and I. N. Sneddon, "Sample title," *Phil. Trans. Roy. Soc. London*, vol. A247, pp. 529–551, April 1955.

I. INTRODUCTION

TODO - This section introduces the problem we are dealing with and motivates the creation of this tool

II. BACKGROUND

TODO - This section goes over the state of the art on analyzing malware binaries, past work on protocol reverse engineering and available tools.

III. DESIGN

TODO - This section covers the general structure of the tool and the different modules and functionalities implemented.

- Requirements: overview and goals of the tool - Arch: overview and details of each stage - Implementation, with repo and how to use

IV. EVALUATION

TODO - This section covers multiple test cases, including custom programs that we will include in our repository that showcase some easy-to-understand cases we want to show that work, and some others that are real malware found in the wild.

Goal of the eval first. It's about checking functionality, and checking that we detect e.g. all commands we know are at the sample

V. RELATED WORK

TODO decide whether to include this or not - It might fit better in the background

VI. CONCLUSION

TODO - This section offers an overview of the developed tool and the results obtained over the problem we were trying to solve.

A. Future work & limitations

ACKNOWLEDGMENT

TODO