COMPARATIVE ANALYSIS OF BOTNETS AND RANSOMWARE FOR EARLY DETECTION

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

PROBLEM STATEMENT

In this study, we compare the features of ransomware and botnets with WannaCry and Mirai respectively as examples. We also discuss measures to detect and mitigate the threat of these types of malware WannaCry and Mirai respectively as examples. We also discuss measures to detect and mitigate the threat of these types of malware

BACKGROUND

We base our process on methods that are widely used in the field of reverse engineering. These processes have been used successfully on a wide variety of malware.

DATASET AND FEATURES / PROJECT REQUIREMENTS/ PRODUCT FEATURES

Through this study, we aim to learn the following:

- Similarities and differences between botnets and ransomware
- Measures to detect and mitigate the threat of botnets and ransomware.

DESIGN APPROACH / METHODS

We statically analyze Mirai, making use of both the sample (in Ghidra) and the original version's source code (released by the author).

For WannaCry, we statically analyze the sample in Ghidra and then dynamically analyze it in a Windows virtual machine.

RESULTS AND DISCUSSION

In analyzing the malware, we have found that there are many implementation techniques common to both Mirai and WannaCry, despite the obvious differences in origin and target platform.

Platform-dependent factors aside, we have found that many of the differences between the implementation of Mirai and WannaCry are a result of different priorities, with Mirai dependent on persistence and WannaCry only needing to avoid detection long enough to do damage.

SUMMARY OF PROJECT OUTCOME

In analyzing the malware, we have found that there are many implementation techniques common to both malware.

We have also been able to find a large number of reliable methods to detect and mitigate the threat of not only Mirai and WannaCry in specific, but botnets and ransomware in general.

CONCLUSION AND FUTURE WORK

We can conclude that despite their similarities in origin and implementation, one can be distinguished from the other by a variety of factors.

We have also found that though these malware are a major threat, many measures exist to mitigate that threat.

REFERENCES

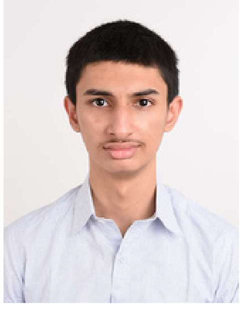
1)O'Kane, P., Sezer, S. & Carlin, D. Evolution of ransomware. IET Networks.7, 321-327 (2018)
2)Sinanovi´c, H. & Mrdovic, S. Analysis of Mirai malicious software. 25th International Conference On Software, Telecommunications And Computer Networks (SoftCOM). pp. 1-5

Authors:

Prof. Prasad B. Honnavalli

Prof. Sushma E.

Achyuta KN



Aditya Rao

Varun S Girimaji

Vrinda S Girimaji