DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

"Botnet Battlefield": A structured study of behavioral interference between different malware families.

Bishwa Hang Rai

DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

"Botnet Battlefield": A structured study of behavioral interference between different malware families.

"Botnet Battlefield": Eine strukturierte Fallstudie über Verhaltnsinterferer zwischen verschiedenen Malware Familien.

Author:	Bishwa Hang Rai
Supervisor:	Prof. Dr. Alexander Pretschner
Advisor:	M.Sc. Tobias Wüchner
Submission Date:	February 15, 2016

I confirm that this master's thesis in informatics is my own work and I have documented all sources and material used.

Munich, February 15, 2016 Bishwa Hang Rai

Acknowledgments

Abstract

Malware of different families may not like each other. For example, different malware binaries might try to uninstall each other before infecting a system. This is an interesting case of 'environment-sensitive malware'. There are some anecdotal evidences (blogs). To the best of our knowledge, there is no prior research addressing this problem in a systematic way. In this research we systematically try explore the scene in the wild. We ran multiple malware samples from different families at the same time in the Anubis environment (a dynamic full-system-emulation-based malware analysis environment). We later analyzed the results of the emulation and detect such behaviors. We used clustering algorithm to cluster the malware based on its resources activities such as file,registry,section,syncs. With this apporach we could find 30 paris of malware that were indeed battling each other. :)

Contents

1 Introduction

1.1 Section

Citation test [Lam94].

1.1.1 Subsection

See Figure 1.1.

Figure 1.1: An example for a figure.

1.2 Section

See Table 1.1, Figure 1.2, Figure 1.3, Figure 1.4.

Table 1.1: An example for a simple table.

A	B	C	D
1	2	1	2
2	3	2	3

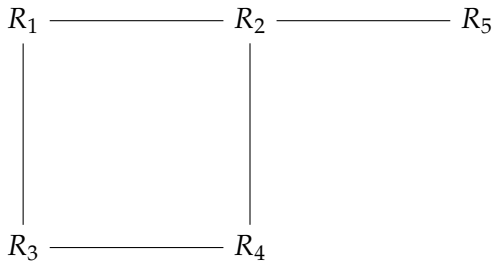

Figure 1.2: An example for a simple drawing.

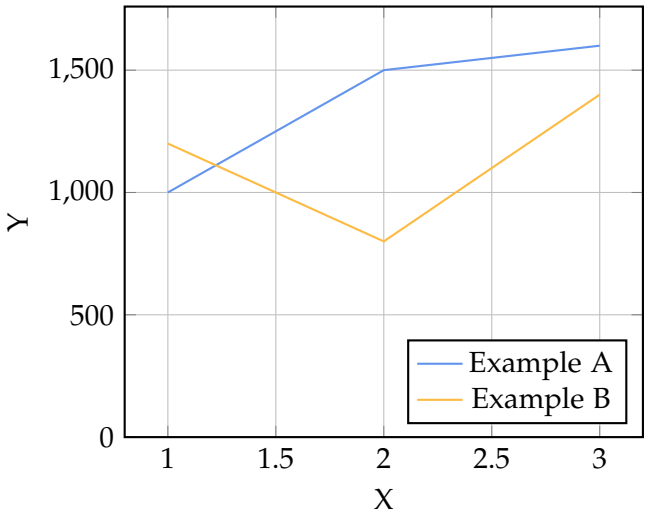

Figure 1.3: An example for a simple plot.

```
SELECT * FROM tbl WHERE tbl.str = "str"
```

Figure 1.4: An example for a source code listing.

List of Figures

List of Tables

Bibliography

[Lam94] L. Lamport. *LaTeX : A Documentation Preparation System User's Guide and Reference Manual*. Addison-Wesley Professional, 1994.