

CONTENTS

1.	Introduction.	_____	01
2.	Overview of Malwares.		
	• Important definitions.	_____	03
	• Different categories.		
	○ Virus.	_____	04
	○ Worms.	_____	04
	○ Trojan horse.	_____	04
	○ Internet worms.	_____	04
3.	An overview of code analysis.		
	• Static analysis.	_____	07
	• Dynamic analysis.	_____	09
	○ Types of dynamic analysis.	_____	10
	• Static analysis vs. dynamic analysis	_____	11
4.	Taint analysis		
	• Tainting data	_____	12
	• Dynamic Taint Analysis	_____	13
	○ ISA categories:	_____	13
5.	The Proposed System		
	• DFD	_____	18
6.	Implementation details		
	• CFG generation and pruning.	_____	19
	• Dynamic taint analysis	_____	27
	• Static execution trace analysis.	_____	30
7.	Conclusion and Future Works.	_____	36
8.	REFERENCES.	_____	37
9.	APPENDIX I.	_____	40
10.	APPENDIX II.	_____	42