

**ENHANCING HONEYPOT TO COLLECT CLIENT SIDE
ATTACKS BEHAVIOR FROM MALICIOUS URL**

By

Jeffry Hirawan

11302021



SWISS GERMAN UNIVERSITY

The Prominence Tower

Jalan Jalur Sutera Barat No.15, Alam Sutera

Tangerang, Banten 15143 - Indonesia

August 2017

Revision after Thesis Defense on 19th July 2017

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Jeffry Hirawan

Date

Student

Approved by:

Charles Lim, M.Sc.

Date

Thesis Advisor

Ir. Heru Purnomo Ipung, M.Eng

Date

Thesis Co-Advisor

Dr.Ir. Gembong Baskoro, M.Sc.

Dean

Date

Jeffry Hirawan



ABSTRACT**Enhancing Honeypot to Collect Client Side Attacks Behavior
from Malicious URL**

By

Jeffry Hirawan

Charles Lim, M.Sc., Advisor

Ir. Heru Purnomo Ipung, M.Eng. Co-advisor

SWISS GERMAN UNIVERSITY

Users are in danger of getting hit by a client side attacks which can come from a malicious URL. This URL can contain trojan apps that disguise as a normal application or trigger a download and executing malware without the user's consent. The research tackled the issue of malicious URL behaviors when interacting with user's system. The Interaction is captured by using a combination of low interaction and high interaction honeypots. Low interaction honeypot will capture site behavior when visited, and capture their malicious payload, while high interaction honeypot collects state changes that occur in user's system during site's visitation. From this research, we can conclude that malicious site can distribute malware by disguising it as a normal application, and some site will behave differently to avoid being detected while being analyzed by the honeypots. We also added improvements to low interaction honeypot by adding the ability to crawl and process a large number of URL automatically. This improvement will improve the capability of the honeypot to gather a large amount of data in a shorter time than before. We have decreased the overall time of the process using this improvement up to 43%.

Keywords: Honeypot, Malicious URL Behavior, client site attacks.



SWISS GERMAN UNIVERSITY

DEDICATION

I dedicate this works for my parents that have supported me in their entire life. Their love and support have let me get this far and I truly thank them for their support.



ACKNOWLEDGEMENTS

I wish to thank the **members of my family** for their support and encouragement during this research. **Mr. Charles Lim** and **Mr. Heru Purnomo Ipung** help were crucial in finishing this research. Their advice and research direction help me finish this research and making time in their busy schedule to help me with this research. Thank you, **Michelle Lioe** for the moral support during hard times while doing this research. Finally, **Tommy Winarta** was very helpful during my coding problem-solving process.



TABLE OF CONTENT

STATEMENT BY THE AUTHOR	2
DEDICATION	5
ACKNOWLEDGEMENTS	6
TABLE OF CONTENT	7
LIST OF FIGURES	9
LIST OF TABLES	10
CHAPTER 1 - INTRODUCTION.....	11
1.1 Background.....	11
1.2 Research Problems	12
1.3 Research Objectives	13
1.4 Research Question	13
1.5 Significant of Study.....	13
1.6 Research Scope.....	13
1.7 Hypothesis	14
CHAPTER 2 - LITERATURE REVIEW	15
2.1 Internet	15
2.2 Development of Internet Threats	15
2.3 Type Security Threats	16
2.3.1 Botnets.....	16
2.3.2 DDoS (Denial-of-service)	17
2.3.3 Malware.....	18
2.3.4 Pharming.....	18
2.3.5 Phising	18
2.4 Increasing Risk Of Cyber Crime.....	18
2.5 Malware	19
2.5.1 Trojans	19
2.5.2 Worms.....	20
2.5.3 Viruses	20
2.5.4 Spyware, Adware, and Other types of misleading software.....	21
2.6 Client side attack Technique	21
2.7 Malware and Distribution Strategies	22
2.7.1 Drive By Download.....	22
2.7.2 Email.....	23
2.7.3 Network Intrusion.....	23
2.7.4 Social Engineering.....	24

2.8 Honeybots	24
2.8.1 Client Side Honeypot	25
2.8.2 Server Side Honeybots	26
2.8.3 Client Honeypot VS Server Honeypot	26
2.8.4 Signature based VS Integrity Check.....	27
2.8.5 Thug Low Interaction Honeypot	28
2.8.6 Capture-HPC Interaction Honeypot	29
2.9 Malicious Invisibility Techniques	31
2.9.1 Anti Crawling Techniques	31
2.9.2 Virtual Environment Detection.....	31
2.9.3 Geo-Location Attacks	31
2.9.4 IP Blacklisting	31
2.9.5 Obfuscation and Redirection	32
2.10 Related Work.....	32
2.11 Contribution	34
CHAPTER 3 – RESEARCH METHODS	35
3.1 Research Methodology	35
3.2 System Overview.....	36
3.3 Research Methodology	36
3.3.1 Enhancement Evaluation Framework.....	37
3.3.2 Information Collection Framework	38
3.3.3 Crawler Module Workflow	40
CHAPTER 4 – EXPERIMENT ANALYSIS	42
4.1 Enviroment Preperation.....	42
4.2 Enhancing Thug – Low Interaction Honeybots.....	43
4.2.2 Queuer Module	47
4.3 Thug Enhancement Evaluation.....	49
4.4 Thug Information Collection Enhancement	51
4.5 Malicious URL Behavior Analysis	52
4.5.1 Distribute Malware	53
4.5.2 Dead Website	54
4.5.3 Infinite Loops	56
4.5.4 Phishing site.....	58
4.6 Captured Malicious Payload.....	60
4.7 Reporting Interface	64
CHAPTER 5 – CONCLUSION	68
5.1 Future Works	70
Bibliography	71
GLOSSARY	73
Appendix.....	74
CURRICULUM VITAE	76