ENHANCING HONEYPOT TO COLLECT CLIENT SIDE ATTACKS BEHAVIOR FROM MALICIOUS URL

By

Jeffry Hirawan

11302021

BACHELOR'S DEGREE

in

INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

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

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 concent. 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.

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