DETECTING ADVANCED PERSISTENT THREAT ATTACK BASED ON DNS NETWORK TRAFFIC USING BAYESNET ALGORITHM

By

Irfan Husein Al Darodjat

12112016

BACHELOR'S DEGREE

in

INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY

SWISS GERMAN UNIVERSITY
EduTown BSDCity
Tangerang 15339
Indonesia

February 2017

DETECTING ADVANCED PERSISTENT THREAT ATTACK BASED ON DNS NETWORK TRAFFIC USING BAYESNET ALGORITHM

By

Irfan Husein Al Darodjat

12112016

BACHELOR'S DEGREE

in

INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY

SWISS GERMAN UNIVERSITY
EduTown BSDCity
Tangerang 15339
Indonesia

February 2017

Revision after the Thesis Defense on 26 January 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 this thesis.

Irfan Husein Al Darodjat
____________________________ ____________
Student Date

SGU® SWISS GERMAN UNIVERSITY

Approved by:

Charles Lim, MSc., ECSA, ECSP, ECIH, CEH, CEI
____________________________ ____________
Thesis Advisor Date

Dr. Ir. Lukas, MAI, CISA, IPM
____________________________ ____________
Thesis Co-Advisor Date

Dr. Ir. Gembong Baskoro, M.Sc
____________________________ ____________
Dean Date

ABSTRACT

DETECTING ADVANCED PERSISTENT THREAT ATTACK BASED ON DNS NETWORK TRAFFIC USING BAYESNET ALGORITHM

By
Irfan Husein Al Darodjat
Charles Lim, MSc., ECSA, ECSP, ECIH, CEH, CEI, Advisor
Dr. Ir. Lukas, MAI, CISA, IPM, Co-Advisor

SWISS GERMAN UNIVERSITY

SGU® SWISS GERMAN UNIVERSITY

A new class of threats, known as Advanced Persistent Threats (APTs), has drawn increasing attention from researchers, primarily from the industrial security sector. APTs are cyber attacks executed by sophisticated and well-resourced adversaries targeting specific information in high-profile companies and governments. This research proposed a mechanism to detect APT threat based on DNS traffic using BayesNet classification algorithm. The validation of the classification is performed. The system successfully achieve 99.6% correctly classified instance. From 4 weeks of student and staff traffic, 223 true APT was found. This result means APT Threat exist in Swiss German University (SGU) DNS server. Feature of APT also can be found in DNS traffic. This research is a precursor in SGU highlighting the directions for future research of APT detection.

Keywords: advanced persistent threat, APT, sophisticated attacks, classification, DNS, machine learning, data mining

SWISS GERMAN UNIVERSITY

© Copyright 2017
By Irfan Husein Al Darodjat
All rights reserved

DEDICATION

To my parents, my campus and for the future of my country: Indonesia

SWISS GERMAN UNIVERSITY

ACKNOWLEDGEMENTS

In the name of God, the Most Gracious, the Most Merciful and may Allah send blessings and peace upon Prophet Muhammad SAWW and the family of Muhammad.

First, I would like to deliver my sincere gratitude to my advisor, Mr. Charles Lim, and my co advisor Mr. Lukas, for the limitless support and time during my thesis research, for their patience, motivation, and immense knowledge. Their knowledge and guidance help me in all the time of research and writing of this thesis and related researches.

Then, I would like to thank all of IT Department of Swiss German University. Lecturers and staffs, Mr. Kho, Mr. Maula, Mr James, Michael who helped me to pass OFSE, Mrs. Mawar, and many others, for all their helps during my study in Swiss German University.

Also, I would like to thank all of seniors and friends in IT SGU, during this research development. For the support and knowledge that help me complete this research. Especially Kris, Mario, Aldi, and Garuda Solusi Kreatif company help me a lot providing the resources for this research.

Lastly, I would like to express my wholehearted thanks to my family for their generous support throughout my entire life. Because of their unconditional love and prayers, i have the strength to complete my bachelor degree.

SWISS GERMAN UNIVERSITY

TABLE OF CONTENTS

SGU ® SWISS GERMAN UNIVERSITY

SWISS GERMAN UNIVERSITY

SWISS GERMAN UNIVERSITY