Ing. Karel Bartoš, Ph.D.
Cisco Systems
Karlovo náměstí 10
Praha 2
kbartos@cisco.com

In Prague, June 8, 2017

OPPONENT'S REPORT – BACHELOR THESIS

Title: Detection of HTTPS Malware Traffic

Student: František Střasák

In Detection of HTTPS Malware Traffic, František focuses on detecting HTTPS malware without decrypting the content of the network communication. Instead, František proposes and combines features extracted from Bro Intrusion Detection System and uses them for classification of malicious and legitimate traffic.

The first chapter of the thesis introduces the thesis as such, while the second chapter deals with the brief discussion of the state of the art methods and emphasizes the novelty of the proposed work. The third chapter describes the type of input data and the datasets used for further analysis and experiments. The forth chapter is the core of the thesis and describes the proposed algorithm for aggregating the input data into groups, followed by the details about the features extracted from these groups. The fifth chapter provides an overview of four classification methods used in the experimental evaluation. Next three chapters evaluate the proposed approach including the classification of malware certificates. The ninth chapter concludes the thesis and outlines the future work.

In general, I have a very positive impression about the thesis. Detecting HTTPS malware traffic without decrypting the content of the communication is very complicated and ambitious problem. František did an excellent job when designing and combining the features and building the classification system. There were some places within the thesis that I would have liked to have seen some additional detail so that I could more adequately judge the results. For example I am missing some discussion for Figures 6.1 and 6.2. In the future work, František proposes to use more information acquired from Bro logs which I think will be necessary in order to increase the feature space and further improve the efficacy of the classification system.

I do recommend the thesis for presentation and my suggested grade is A – excellent.

Ing. Karel Bartoš, Ph.D.