ČESKÉ
VYSOKÉ
UČENÍ
TECHNICKÉ
V PRAZE

SUPERVISOR‘S OPINION OF FINAL THESIS

I. IDENTIFICATION DATA

Thesis name:	Behavioral Analysis and Detection of IoT malware using the IRC protocol
Author’s name:	**Ondrej Prenek**
Type of thesis :	Master Thesis
Faculty/Institute:	Faculty of Electrical Engineering
Department:	Computer Science
Thesis supervisor:	Sebastian Garcia
Supervisor’s department:	Computer Science

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment	**Ordinarily Challenging**

Evaluation of thesis difficulty of assignment.

The topic of the thesis is challenging from the point of view that the IRC protocol is designed for human chat interaction and not a common and control, therefore it was expected to be challenging to detect.

Satisfaction of assignment	**Fulfilled**

Assess that handed thesis meets assignment. Present points of assignment that fell short or were extended. Try to assess importance, impact or cause of each shortcoming.

The work was completely fulfilled to the expectations

Activity and independence when creating final thesis	**B. Very Good**

Assess that student had positive approach, time limits were met, conception was regularly consulted and was well prepared for consultations. Assess student’s ability to work independently.

The student met the limits, and consulted regularly.

Technical level	**B. Very good**

Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by experience.

The level of thesis speciality, language and study of expert literature, sources and data were very good.

Formal and language level, scope of thesis **B. Very good**

Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.

The thesis has the correct usage of formal notation and language.

Selection of sources, citation correctness **A. Excellent**

Present your opinion to student's activity when obtaining and using study materials for thesis creation. Characterize selection of sources. Assess that student used all relevant sources. Verify that all used elements are correctly distinguished from own results and thoughts. Assess that citation ethics has not been breached and that all bibliographic citations are complete and in accordance with citation convention and standards.

All the important references are included and the sources and citations were done correctly.

Additional commentary and evaluation

Present your opinion to achieved primary goals of thesis, e.g. level of theoretical results, level and functionality of technical or software conception, publication performance, experimental dexterity etc.

The thesis achieved its goals with results that are level with the expectation of the task. The solutions were applied and had a performance that was good for an experimental setup. The solution was implemented in working code that is part of a real solution.

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

Overall the thesis was fulfilled and demonstrated that is possible to detect a command and control channel when is implemented in IRC. It also analyses the behavioural characteristics of the protocol, where some expected limitations are confirmed, contributing the knowledge to the area. The implementations done for the Zeek intrusion detection system were paramount and complex, being valuable for the community.

I evaluate handed thesis with classification grade **B**

Date: **Aug, 22th, 2020** Signature: