Bachelor thesis opponent’s review

Master thesis: Execution, Analysis and Detection of Android RATs traffic
Author: Babayeva Kamila
Thesis supervisor: Ing. Sebastián García, Ph.D.
Thesis opponent: Ing. Martin Grill, Ph.D.

Rating (1 – 5)
(1 = best; 5 = worst):

1. Fulfillment of assignment requirements: 1
2. Systematic solutions of individual tasks: 2
3. Ability to apply knowledge and to use literature: 1
4. Thesis formal and language level: 1
5. Thesis readability and structuring: 1
6. Thesis professional level: 1
7. Conclusions and their formulation: 2
8. Final mark evaluation (A, B, C, D, E, F): verbal:Excellent

Brief summary evaluation of the thesis (compulsory):

The proposed bachelor thesis provides a detailed analysis of network traffic generated by Android Remote Access Trojans. Student was able to acquire, install and execute available commands of eight different RATs within a well-prepared testing environment. All the captured traffic generated by the RATs was analyzed, thoroughly documented and published so it can be easily used by other security researchers. Student also introduced and evaluated five different simple RAT detection methods. The implementations are provided to the community as open source. Formally, the thesis is well written with a clear structure and minimal number of typos.

Questions:

1. The evaluation of the proposed detection methods could be improved as it currently includes only comparison to a legitimate behavior generated in Linux OS. How does the RAT network traffic compare to a traffic generated by some legitimate network-exploiting Android application or game?
2. Are there any false positives of the proposed detection method when analyzing network traffic of an Android phone with a commonly installed set of applications?

Date: 10.6.2021
Signature: