FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Supervisor:	Ing. Josef Kokeš, Ph.D.
Student:	Bc. Matěj Havránek
Thesis title:	Attacks on Event Tracing for Windows: Techniques and Countermeasures
Branch / specialization:	Computer Security
Created on:	12 May 2023

Evaluation criteria

1. Fulfillment of the assignment

▸ [1] **assignment fulfilled**
[2] assignment fulfilled with minor objections
[3] assignment fulfilled with major objections
[4] assignment not fulfilled

The assignment was completed in its entirety, which is quite an achievement considering how complex it was.

2. Main written part

100 / 100 (A)

The written part is excellent. The text is very detailed, but compact and at the same time easy to read and understand. It is well structured and follows a logical sequence. I did not notice any factual errors. Both the typographical level and the language used are nearly perfect. External sources are properly cited.

3. Non-written part, attachments

100 / 100 (A)

There are several non-written components in this thesis. The reader will receive a set of applications to demonstrate the different types of attacks as well as tools able to detect such attacks in a realistic environment. A very significant part of the thesis is also the under-the-hood analysis of actual malware which was crucial for understanding the techniques used and developing countermeasures. I would like to stress that we are talking kernel-mode code here, which is generally poorly (or not at all) documented and difficult to analyze.

4. Evaluation of results, publication outputs and awards 100 /100 (A)

The thesis represents an excellent study material for the subject area covered in it. It builds upon existing results and expands them significantly. both in the analysis of already known techniques (albeit known only to malware developers, not their opponents) and in the possible countermeasures. I consider these results of very high value especially to antimalware developers. I expect a publication will be eagerly accepted by any security-related conference.

5. Activity of the student

[1] excellent activity
[2] very good activity
▸ **[3] average activity**
[4] weaker, but still sufficient activity
[5] insufficient activity

The student was about as active as could be expected. For the most part he worked independently but when there was a reason to discuss something, he was always well prepared and able to explain the topic or ask relevant questions.

6. Self-reliance of the student

▸ **[1] excellent self-reliance**
[2] very good self-reliance
[3] average self-reliance
[4] weaker, but still sufficient self-reliance
[5] insufficient self-reliance

The overall evaluation 100 /100 (A)

The student prepared an exceptional thesis. He chose a very challenging topic that few would be able to approach and handled it quite admirably. The amount of work stored in the thesis is staggering as a significant amount of information had to be extracted from malware and/or undocumented kernel code. I am still amazed that the student was able to complete all the goals he set out to complete, do it on time and in such a high quality. This is beyond any doubt one of the best theses I have seen so far. I grade the thesis A-excellent and recommend that it be considered for the Dean's Award.

Instructions

Fulfillment of the assignment

Assess whether the submitted FT defines the objectives sufficiently and in line with the assignment; whether the objectives are formulated correctly and fulfilled sufficiently. In the comment, specify the points of the assignment that have not been met, assess the severity, impact, and, if appropriate, also the cause of the deficiencies. If the assignment differs substantially from the standards for the FT or if the student has developed the FT beyond the assignment, describe the way it got reflected on the quality of the assignment's fulfilment and the way it affected your final evaluation.

Main written part

Evaluate whether the extent of the FT is adequate to its content and scope: are all the parts of the FT contentful and necessary? Next, consider whether the submitted FT is actually correct – are there factual errors or inaccuracies?

Evaluate the logical structure of the FT, the thematic flow between chapters and whether the text is comprehensible to the reader. Assess whether the formal notations in the FT are used correctly. Assess the typographic and language aspects of the FT, follow the Dean's Directive No. 52/2021, Art. 3.

Evaluate whether the relevant sources are properly used, quoted and cited. Verify that all quotes are properly distinguished from the results achieved in the FT, thus, that the citation ethics has not been violated and that the citations are complete and in accordance with citation practices and standards. Finally, evaluate whether the software and other copyrighted works have been used in accordance with their license terms.

Non-written part, attachments

Depending on the nature of the FT, comment on the non-written part of the thesis. For example: SW work – the overall quality of the program. Is the technology used (from the development to deployment) suitable and adequate? HW – functional sample. Evaluate the technology and tools used. Research and experimental work – repeatability of the experiment.

Evaluation of results, publication outputs and awards

Depending on the nature of the thesis, estimate whether the thesis results could be deployed in practice; alternatively, evaluate whether the results of the FT extend the already published/known results or whether they bring in completely new findings.

Activity of the student

From your experience with the course of the work on the thesis and its outcome, review the student's activity while working on the thesis, his/her punctuality when meeting the deadlines and whether he/she consulted you as he/she went along and also, whether he/she was well prepared for these consultations.

Self-reliance of the student

From your experience with the course of the work on the thesis and its outcome, assess the student's ability to develop independent creative work.

The overall evaluation

Summarize which of the aspects of the FT affected your grading process the most. The overall grade does not need to be an arithmetic mean (or other value) calculated from the evaluation in the previous criteria. Generally, a well-fulfilled assignment is assessed by grade A.