

## Posudek oponenta bakalářské práce

**Student:** Voščinář Martin  
**Téma:** Hlubková analýza podobnosti kódu v malware kmenech (id 25140)  
**Oponent:** Kolář Dušan, doc. Dr. Ing., UIFS FIT VUT

- 1. Náročnost zadání** **obtížnější zadání**  
Zadání považuji za obtížnější, neboť vyžaduje získání dodatečných znalostí a dovedností z oblasti reverzního inženýrství a kryptografie.
- 2. Splnění požadavků zadání** **zadání splněno**  
Zadání bylo splněno, práce obsahuje navíc důkladné rozборы několika rodin ransomware. Bod 3 řešení je roztroušen mezi jednotlivými kapitolami a zasloužil by ucelenější popis.
- 3. Rozsah technické zprávy** **je v obvyklém rozmezí**  
Text práce je určitě delší, než je obvyklé, není to však na újmu. Text je ve všech ohledech zajímavý a přináší řadu zajímavých informací.
- 4. Prezentací úroveň předložené práce** **95 b. (A)**  
Kapitoly na sebe vhodně navazují, text je čtivý, přitom zajímavý a informačně bohatý. Na pár místech se vyskytují nějaké drobné neobratnosti, ale bez zásadního vlivu na celkové hodnocení.
- 5. Formální úprava technické zprávy** **85 b. (B)**  
Formálně je práce v pořádku, stran jazyka je pozorovatelných cca 6 překlepů. Dále dojem po formální stránce kazí opakování poznámek pod čarou pro stejné termíny, např. Malpedia.
- 6. Práce s literaturou** **100 b. (A)**  
Podle mě správná volba vzhledem k tématu práce.
- 7. Realizační výstup** **100 b. (A)**  
Výstupem není kód, ale naopak analýza ransomware. Ta byla udělána na vysoké úrovni preciznosti a důkladnosti. Vytvořena byla pravidla pro program YARA, ta splňují všechny náležitosti, dále byla iniciována změna v nástroji YaraZilla.
- 8. Využitelnost výsledků**  
Výsledky - pravidla, opravený nástroj YaraZilla - jsou již aktivně využívány.
- 9. Otázky k obhajobě**  
Nemám, probrali jsem se studentem osobně.
- 10. Souhrnné hodnocení** **100 b. výborně (A)**  
Podle mě špičková práce, která svým obsahem zdaleka přesahuje průměr a jasně vybočuje nad rámec bakalářských prací i po stránce odbornosti. Osobně se domnívám, že v případě příkladné obhajoby by mohla být i oceněna.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 30. května 2022

Kolář Dušan, doc. Dr. Ing.  
oponent