

## Posudek oponenta diplomové práce

**Student:** Jacko Jerguš, Bc.  
**Téma:** Obfuskační techniky ransomware (id 21832)  
**Oponent:** Barabas Maroš, Ing., Ph.D., UITS FIT VUT

- 1. Náročnost zadání** **obtížnější zadání**  
Zadání práce hodnotím jako obtížnější. Student musel věnovat velké úsilí studováním odborných zdrojů, využití nastudovaných informací pro návrh vlastních metod, následně je implementovat a otestovat pomocí proprietárních bezpečnostních řešení. Tématika obfuskační a šifrovací techniky ransomware a jejich detekce patří mezi zložitější oblasti bezpečnosti.
- 2. Splnění požadavků zadání** **zadání splněno**  
Všechny body zadání považuji za splněné.
- 3. Rozsah technické zprávy** **je v obvyklém rozmezí**  
Rozsah technické zprávy je v obvyklém rozmezí.
- 4. Prezentací úroveň předložené práce** **80 b. (B)**  
Technická zpráva je logicky strukturovaná s doboru návazností kapitol. Text je čtivý a pochopitelný pro čtenáře. Závěr práce práce je stručnější, dosažené výsledky by si zasloužily větší komentář a diskuzi k možnostem rozšíření.
- 5. Formální úprava technické zprávy** **90 b. (A)**  
Celkově je formální úprava poměrně dobrá bez závažnějších nedostatků. V práci se občas vyskytují překlepy a gramatické chyby.
- 6. Práce s literaturou** **100 b. (A)**  
V seznamu literatury jsou publikace, které jsou relevantní k obsahu práce, výběr studijních materiálů je vyvážený, na textu i v literatuře je vidět velký záběr studovaných zdrojů. Práce s citacemi je kvalitní.
- 7. Realizační výstup** **90 b. (A)**  
Student předvedl kvalitní práci při realizaci programového řešení. Výstup včetně zdrojového kódu je kvalitně spracován a zdokumentován. V dokumentační části práce lze vytknout jen menší rozsah analýzy a návrhu řešení, naopak musím vyzdvihnout kvalitně spracovanou teoretickou část a samotné testování.
- 8. Využitelnost výsledků**  
Výsledky práce jsou využitelné v zvýšení bezpečnosti anti-ransomware nástrojů a antivirových metod. Práce přináší využití různých metod obfuskační pro zamezení nebo snížení účinnosti detekce ransomware. Tyto poznatky mohou být využity pro úpravu stávajících metod detekce a zvýšení jejich účinnosti.
- 9. Otázky k obhajobě**  
Bez otázek.
- 10. Souhrnné hodnocení** **90 b. výborně (A)**  
Zadání práce vyžadovalo pečlivé nastudování problematiky obfuskační kódu v kombinaci s oblastmi kryptografie, detekce ransomware, ale také programování netriviálních algoritmů. Student zvládl všechny body zadání a do práce zakomponoval i vlastní využití metody white-box kryptografie. Textová část práce obsahuje menší nedostatky popsány v předchozích bodech hodnocení. Celkově hodnotím práci studenta výjimečným bodovým hodnocením **90 A**.

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

V Brně dne: 6. června 2019

Barabas Maroš, Ing., Ph.D.  
oponent