Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK VEDOUCÍHO DIPLOMOVÉ PRÁCE

Student: **Bc. Václav Hess** **Vedoucí práce:** **Ing. Milan Oulehla, Ph.D.**

Studijní program: **Informační technologie**
Studijní obor/Specializace: **Kybernetická bezpečnost**
Akademický rok: **2021/2022**

Téma diplomové práce: **Charakteristiky moderního malwaru**

Hodnocení práce:		**A**	**B**	**C**	**D**	**E**	**F**
		Hodnocení: A – nejlepší; F - nevyhovující					
1.	Splnění všech bodů zadání	☒	☐	☐	☐	☐	☐
2.	Vhodnost zvolené metody řešení	☒	☐	☐	☐	☐	☐
3.	Členění práce (kapitoly, podkapitoly, odstavce)	☒	☐	☐	☐	☐	☐
4.	Práce s literaturou a její citace	☒	☐	☐	☐	☐	☐
5.	Úroveň jazykového zpracování	☐	☒	☐	☐	☐	☐
6.	Formální úroveň práce	☐	☒	☐	☐	☐	☐
7.	Kvalita zpracování teoretické části	☒	☐	☐	☐	☐	☐
8.	Kvalita zpracování praktické části	☒	☐	☐	☐	☐	☐
9.	Dosažené výsledky práce	☒	☐	☐	☐	☐	☐
10.	Přínos práce a její využití	☒	☐	☐	☐	☐	☐
11.	Spolupráce autora s vedoucím práce	☒	☐	☐	☐	☐	☐

Výsledek kontroly plagiátorství:
Práce byla posouzena z hlediska plagiátorství s výsledkem 1% shodnosti. Práce není plagiát.

Celkové hodnocení práce:
Výsledná známka není průměrem výše uvedených hodnocení. Známku uvede vedoucí dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Další připomínky, vyjádření, náměty k obhajobě práce (možno pokračovat i na další stránce):
Student pravidelně konzultoval zpracování jednotlivých částí závěrečné práce a připomínky vedoucího práce zapracovával.

Těžiště práce spatřuji především v praktické části, která se zabývá analýzami rodin malwarů a identifikací charakteristik malwaru, které mají detekční potenciál. O kvalitě práce svědčí skutečnost, že autor na základě zjištěných charakteristik vytvořil YARA pravidla, která prakticky ověřil.

Nicméně za nejpřínosnější část práce považuji část, která se zabývá softwarovými nástroji použitelnými pro analýzu moderního malwaru. Vytvoření této části práce bylo velmi časově náročné, neboť to vyžadovalo:

1. výběr vhodných nástrojů na základě studia dostupných literárních pramenů,
2. instalaci a konfiguraci vybraných nástrojů,
3. osvojení si používání daných nástrojů,
4. pořízení snímků, zachycující typický příklad použití demonstrovaných nástrojů.

Uvedená část práce může dobře posloužit začínajícím bezpečnostním odborníkům, kteří se chtějí zabývat analýzou malwaru.

Jediným nedostatkem je výskyt několika formulací, které jsou z jazykového hlediska poněkud těžkopádné. Nicméně je potřeba zdůraznit, že se jedná o drobnosti, které nemají vliv na odbornou kvalitu práce.

Závěrečná práce formálně i obsahově splňuje všechny body zadání, lze ji proto doporučit k obhajobě.

Otázka:
Část práce, která se zabývá softwarovými nástroji použitelnými pro analýzu moderního malwaru, může být velmi přínosná pro bezpečnostní komunitu, máte s touto částí práce nějaké další plány?

Datum 24. 5. 2022 Podpis vedoucího diplomové práce