Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **BC. HESS VÁCLAV** **Oponent:** **Ing. Ladislav Vyskočil**

Studijní program: **Inženýrská informatika**
Studijní obor/Specializace: **Kybernetická bezpečnost**
Akademický rok: **2021/2022**

Téma diplomové práce: **Charakteristiky moderního malwaru**

Hodnocení práce:

Cílem diplomové práce bylo popsat problematiku charakteristik moderního malwaru, k jehož dosažení bylo třeba naplnit několik bodů, jejichž přesná specifikace byla součástí zásad uvedených v zadání práce. Všechny body zadání diplomové práce byly splněny v plném rozsahu. Diplomant popisované problematice velmi dobře rozumí. Náročnost a rozsah diplomové práce je nadstandardní. Z obsahu práce vyplývá, že diplomant má s analýzou malwaru rozsáhlé zkušenosti.

Diplomová práce je přehledně strukturována a jednotlivé části na sebe logicky navazují. Text práce je zpracován srozumitelně. Po jazykové stránce nebyly nalezeny žádné pravopisné, nebo stylistické chyby. Po formální stránce je práce vhodným způsobem řazena do logických celků a doplněna upřesňujícími komentáři i odkazy na odpovídající literární či elektronické zdroje. V diplomové práci autor uvádí přiměřené množství obrázků, tabulek a příloh k objasnění popisované problematiky.

V teoretické části byl popsán současný stav řešené problematiky včetně recenzí doporučené literatury, byly pečlivě rozebrány typy a analýzy malwaru, detailně byly popsány i maskovací techniky malwaru. Dále byl popsán rozsáhlý seznam softwarových nástrojů, které lze využít na analýzu malwaru, kdy funkcionalita a použití každého nástroje je podrobně popsána s praktickou ukázkou ve formě obrázku. Závěr teoretické části se zabývá vyhodnocením a srovnáním jednotlivých softwarových nástrojů. Obsah teoretické části odpovídá požadavkům aplikační praxe.

Praktická část se zabývá analýzou první a druhé rodiny vzorků malwaru, za použití nástrojů uvedených v teoretické části diplomové práce, k získání významných charakteristik malwaru, které mohou sloužit k jejich detekci. Postup jednotlivých statických a dynamických analýz včetně disassemblingu byl podrobně a přehledně popsán včetně obrazové dokumentace získaných výstupů a srozumitelné interpretace výsledků analýz. Pro účely detekce byly vytvořeny unikátní YARA pravidla. Závěrem praktické části bylo popsání a vyhodnocení množiny charakteristik současného malwaru, které mají detekční potenciál.

Přínosem práce je podrobný a srozumitelný popis dané problematiky s praktickými ukázkami, které lze použít jako vzorové postupy analýz malware v praxi.

Diplomová práce se jeví jako velmi zdařilá a splňující svůj cíl, a proto ji doporučuji předložit k obhajobě.

Otázka k obhajobě: Uvažujete se v budoucnosti touto problematikou dále zabývat?

Celkové hodnocení práce:
Známku uvede oponent 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.

Datum 1. 6. 2022 Podpis oponenta diplomové práce