

Posudek práce

předložené na Přírodovědecké fakultě JU

☒ posudek vedoucího
☐ bakalářské práce

☐ posudek oponenta
☒ diplomové práce

Autor/ka: Bc. Martin Kunc

Název práce: Dynamická analýza malware s cílem získávání indikátorů kompromitace a jejich následného využití

Studijní program a obor: Aplikovaná informatika

Rok odevzdání: 2019

Jméno a tituly vedoucího/opponenta: Ing. Petr Břehovský

Pracoviště: Ústav aplikované informatiky

Kontaktní e-mail: pbrehovsky@prf.jcu.cz

Odborná úroveň práce:

☐ vynikající ☒ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

Věcné chyby:

☒ téměř žádné ☐ vzhledem k rozsahu přiměřený počet ☐ méně podstatné četné ☐ závažné

Výsledky:

☒ originální ☐ původní i převzaté ☐ netriviální kompilace ☐ citované z literatury ☐ opsané

Rozsah práce:

☐ veliký ☒ standardní ☐ dostatečný ☐ nedostatečný

Grafická, jazyková a formální úroveň:

☐ vynikající ☒ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

Tiskové chyby:

☐ téměř žádné ☒ vzhledem k rozsahu a tématu přiměřený počet ☐ četné

Celková úroveň práce:

☐ vynikající ☒ velmi dobrá ☐ průměrná ☐ podprůměrná ☐ nevyhovující

Slovní vyjádření, komentáře a připomínky vedoucího:

Práce podrobně popisuje proces získávání a analýzy škodlivého kódu pomocí dostupných prostředků. Škodlivý kód je získáván z reálných honeypotů provozovaných sdružením CZ.NIC. V práci jsou analyzována dvě běžná prostředí pro analýzu škodlivého kódu se závěrem, že je nutné vytvořit prostředí vlastní, které je podrobně popsáno. Je popsán proces analýzy škodlivého kódu, který je vzhledem k velkému množství vzorků nutné automatizovat. Značný prostor je věnován analýze, třídění a popisu analyzovaných vzorků. Zadání práce bylo bezezbytku splněno s tím, že bylo dosaženo několika dalších cílů. Byly identifikovány dosud neznámé vzorky škodlivého kódu. Výsledky práce posloužily jako vstupní data pro projekty Turris a PROKI, nebo jako včasné varování před útoky na infrastrukturu státu. Práce může sloužit jako návod ke sběru a analýze škodlivého kódu, který mohou použít i méně zkušení analytici. Výsledky práce byly publikovány na odborné konferenci a v tisku.

Případné otázky při obhajobě a náměty do diskuze:**Práci**

☒ doporučuji
☐ nedoporučuji
uznat jako diplomovou.

Navrhuji hodnocení stupněm:

☒ výborně ☐ velmi dobře ☐ dobře ☐ neprospěl/a

20.5.2019 

Místo, datum a podpis vedoucího/oponenta:
V Českých Budějovicích