Posudek práce

předložené na Přírodovědecké fakultě JU

☑ posudek vedoucího ❑ posudek oponenta
❑ bakalářské práce ☑ diplomové práce

Autor/ka: Jaroslav Kovář
Název práce: Analýza škodlivého kódu ve virtuálním prostředí
Studijní program a obor: Aplikovaná informatika
Rok odevzdání: 2019

Jméno a tituly vedoucího: ing. Petr Břehovský
Pracoviště: ÚAI PřF Jihočeská univerzita, České Budějovice
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 spočívá ve vytvoření virtuálního prostředí pro analýzu malware, které podporuje antievasivní techniky analytických nástrojů inspirované biologií (mutace a použití technik útočníka proti němu samotnému). Testovacími evasivními programy je prostředí porovnáno s běžným virtuálním prostředím a je tak potvrzena jeho nízká detekovatelnost. Prostředí je dále použito k analýze skutečného malware.
Je nutné vyzdvihnout originální způsob ovládání analytických nástrojů pomocí simulace stisku kláves z vněšku prostředí, který škodlivému kódu výrazně ztěžuje detekci prostředí a zároveň generuje uživatelskou aktivitu, kterou některé škodlivé kódy testují.
Práce představuje velký objem vynaložené práce (analýza evasivních technik, návrh opatření proti nim, příprava několika různorodých prostředí, analýza nástrojů, analýza jiných prostředí pro zkoumání škodlivého kódu, analýza threat inteligence, příprava knihovny testovacího malware a v neposlední řádě implementace antievasivních technik, otestování vytvořených prostředí a analýza vybraného škodlivého kódu). Text práce je přehledný, dobře strukturovaní, s mnoha odkazy na literaturu a pro středně pokročilé analytiky přínosný.

Případné otázky při obhajobě a náměty do diskuze:

Práci
☑ doporučuji
☐ nedoporučuji
uznat jako diplomovou.

Navrhuji hodnocení stupněm:
☑ výborně ☐ velmi dobře ☐ dobře ☐ neprospěl/a

Místo, datum a podpis vedoucího/oponenta:
V Českých Budějovicích 8.1.2020