FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jakub Souček
Student:	Matěj Havránek
Název práce:	Deobfuskace malware v jazyce VBScript
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	21. května 2021

Hodnotící kritéria

1. Splnění zadání

▸ [1] **zadání splněno**
[2] zadání splněno s menšími výhradami
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

Student splnil zadání v plném rozsahu. Stanovených cílů bylo dosaženo v dostatečné kvalitě.

2. Písemná část práce 100 / 100 (A)

Práce je dobře strukturovaná a velmi dobře se čte. Licenční podmínky nebyly porušeny.

3. Nepísemná část, přílohy 100 / 100 (A)

Deobfuskátor vytvořený v rámci ZP je velmi kvalitní. Adresuje mnoho obfuskačních technik různého charakteru a poskytuje metody k jejich deobfuskaci. Velmi pozitivně hodnotím fakt, že uživatel je schopen definovat kroky, které se mají vykonat, ať už z příkazové řádky nebo grafického rozhraní - funkcionalita, kterou poskytuje málokterý deobfuskátor. Výhodou také je, že deobfuskátor pracuje nad AST a jediná část, která jej pevně váže s jazykem VBScript, je parser, a je zde tedy poměrně jednoduchá cesta pro integraci dalších scriptovacích jazyků. Kombinací statických deobfuskací a modifikovaného interpreteru jazyka VBScript získává deobfuskátor velmi široký záběr.

4. Hodnocení výsledků, jejich využitelnost 100 / 100 (A)

Univerzální scriptový deobfuskátor, který umožňuje uživateli plně řídit deobfuskační proces a navíc sledovat výsledky jednotlivých kroků, je velmi užitečný nástroj. Analytik malware může tento nástroj použít jak k automatizované deobfuskaci, tak k manuální

hluboké analýze funkcionality. Z vlastní praxe mohu říct, že již v současném stavu má vyvinutý deobfuskátor obrovský přínos pro analýzu scriptového malware.

Celkové hodnocení

100 /100 (A)

Deobfuskace jazyka VBScript je, jak práce zmiňuje, oblast bez existence dostatečně sofistikovaných deobfuskačních nástrojů. Deobfuskátor vyvinutý v rámci ZP nabízí vysoce kvalitní přístup k deobfuskaci jazyka VBScript a navíc pracuje nad AST a nabízí tak půdu pro rozšíření na další scriptovací jazyky.

Otázky k obhajobě

Co Vás vedlo k výběru právě jazyka VBScript?

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.