FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Josef Kokeš
Student:	Matěj Havránek
Název práce:	Deobfuskace malware v jazyce VBScript
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	26. 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

Zadání bylo beze zbytku splněno, vytvořený program je funkční a dobře řeší předmětnou oblast.

2. Písemná část práce 95 / 100 (A)

Text práce přehledně a srozumitelně provádí čtenáře problematikou obfuskovaného malwaru v jazyce VBScript a možnostech jeho deobfuskace. Analýza problémové oblasti je úplná a návrh nástroje pro usnadnění analýzy obfuskovaných skriptů je dobrý a užitečný. Po jazykové stránce jsem zaznamenal příležitostné nesprávné použití členů, ale nebrání to v porozumění práce. Zbytek textu je bez výhrad. Technická stránka odpovídá běžným standardům.

3. Nepísemná část, přílohy 95 / 100 (A)

Vytvořený nástroj je výborným počátečním bodem pro analýzu obfuskovaného malware v VBScriptu. Inspirace nástrojem IDA Pro se nezapře, což je dobře. Nástroj je už ve své první verzi velice účinnou pomůckou analytika, menší nedostatky spatřuji v uživatelském rozhraní (informační okna nelze zavřít pomocí ESC; při spuštění programu z konzolového okna je toto po dobu běhu programu skryto; velké skripty se zpracovávají dlouho bez signalizace uživateli, že program stále žije; dlouho mi trvalo, než jsem našel, že částečné vyhodnocení výrazů je skryté pod tlačítkem Transform).

Kód programu je čistý a přehledný, chybí mi však návod ke kompilaci.

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

Hlavním výstupem práce je program pro interaktivní deobfuskaci skriptů v jazyce VBScript. Jde o vysoce specializovanou oblast, což omezuje možnosti využití, tuto oblast však program řeší už v této verzi výborně a vidím v něm veliký potenciál do budoucna, zejména bude-li rozšířen o další běžné skriptovací jazyky. Na to je svojí konstrukcí připraven.

5. Aktivita studenta

- [1] **výborná aktivita**
  [2] velmi dobrá aktivita
  [3] průměrná aktivita
  [4] slabší, ale ještě dostatečná aktivita
  [5] nedostatečná aktivita

Není co dodat, student byl aktivní.

6. Samostatnost studenta

- [1] **výborná samostatnost**
  [2] velmi dobrá samostatnost
  [3] průměrná samostatnost
  [4] slabší, ale ještě dostatečná samostatnost
  [5] nedostatečná samostatnost

Prakticky celou práci vytvořil student zcela samostatně, což nade vši pochybnost ukazuje, že je schopen samostatné tvořivé práce.

Celkové hodnocení 99 /100 (A)

Práce se zaobírá důležitou a přitom dosud uspojivě systematicky neřešenou problematikou deobfuskace kódů v jazyce VBScript. Jejím výstupem je analýza současného stavu a na ní postavený nástroj, který je platným pomocníkem pro analytika. Po funkcionální stránce je už v této základní verzi výborný, navíc s výhledem na další vylepšení o podporu dalších skriptovacích jazyků. Drobné nedostatky v uživatelském rozhraní budou jistě vychytány v návaznosti na to, jak bude program prakticky používán. Práce si bezpochyby zaslouží hodnocení známkou A-výborně.

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.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

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.