Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Bc. Jan Řečínský
Vedoucí práce: Ing. Josef Kokeš
Název práce: Analýza kryptoviru
Obor: Počítačová bezpečnost

Datum vytvoření: 9. 1. 2016

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	***1=mimořádně náročné zadání,*** *2=náročnější zadání, 3=průměrně náročné zadání, 4=lehčí, ale ještě dostatečně náročné zadání, 5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Student si zvolil mimořádně náročné zadání, a to nejen vůči průměrnému zadání diplomových prací na ČVUT FIT, ale i vůči ostatním mimořádně náročným zadáním. Reverzní analýza programů je téměř vždy velmi obtížná, tím spíše u malwaru, který má všechny důvody pro to, aby se analýze co nejúčinněji bránil. Na to, aby se vůbec někam v analýze dostal, musel vynaložit znalosti a námahu, která jsou výrazně větší, než lze od studenta spravedlivě požadovat.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami, 3=zadání splněno s většími výhradami, 4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Zadání tak, jak je formulováno, bylo splněno. Původní zadání (student obhajobu opakuje) zjevně počítalo s tím, že se podaří odhalit více informací, např. detaily o použitém šifrování nebo identita autora malwaru, vzhledem k vysoké profesionalitě tvůrce CBT-Lockeru však není překvapující, že k tomu nedošlo. Není to naprosto vina studenta.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami, 3=splňuje požadavky s většími výhradami, 4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Není co dodat.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*95 (A)*

Popis kritéria:
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.

Komentář:
Po věcné stránce nemám výhrady, práce je výborná. Možná by jí prospělo, kdyby šla víc do hloubky na úkor šířky, ale i zvolený přístup je zcela legitimní.
Logická stránka je vesměs v pořádku, našel jsem jen dvě problematická místa:
1) Poslední odstavec kapitoly 1.1 nemá na tomto místě smysl (důsledek refaktoringu textu těsně před odevzdáním).
2) Kapitoly 5.2.8-5.4 by logicky měly být podkapitolami kapitoly 5.5.
Tyto nedostatky však nemají vliv na srozumitelnost práce ani její věcnou správnost.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*60 (D)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 12/2014, článek 3.

Komentář:
Formální úroveň práce byla jedním z důvodů, proč jsem ji jako oponent hodnotil jako nedostatečnou. Student na této stránce výrazně zapracoval a za výsledek už se nemusí stydět. V práci se stále nachází jazykové chyby, není jich však nad rámec běžný v jiných pracích a z velké většiny spadají do kategorie překlepů, hrubky a nedokončené odstavce jsou minulostí (až na poznámku pod čarou na straně 48). Práce má ještě rezervy ve slohové stránce, text se ne vždy dobře čte - návaznosti mezi větami či odstavci jsou mnohdy problematické nebo úplně chybí, nicméně nevytrhují ze čtení příliš.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*80 (B)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Také na práci se zdroji je vidět zřetelné zlepšení, materiály jsou nyní relevantní a dobře citované, i když někdy poněkud zvláštně volené (např. v pojednání o TORu bych očekával spíš odkazy na oficiální stránky než na blog třetí osoby). Potěší použití tištěných zdrojů, v předmětné oblasti jich zase tolik k dispozici není. Jako čtenář bych uvítal odkazy na články, které se zabývají rekonstrukcí programu z jeho obrazu v paměti, nejde však o stěžejní problematiku práce.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*100 (A)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Student prokázal vysoce nadstandardní schopnosti v oblasti reverzního inženýrství, daleko nad rámec toho, co po něm bylo možné požadovat. Není pochyb o tom, že bude schopen v oboru pokračovat i v praktickém životě.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Práce má velký handicap v tom, že se zabývá výrazně časově omezenou tematikou, která značně snižuje možnosti publikace: jakmile jednou malware přestane být aktivní, k čemuž došlo zhruba v lednu 2015, budou výsledky obtížně upotřebitelné i v případě, že by se podařilo např. prolomit šifrování souborů a zachránit data (v té době už budou buď odšifrovaná po zaplacení výkupného nebo obnovená z jiných zdrojů). Nicméně jako nástroj pro získání praktických zkušeností s reverse engineeringem má podle mě značnou trvalou hodnotu a dovedu si představit její využití ve výuce reverzního inženýrství.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 9b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:
Student byl velmi aktivní a vždy připravený, není, co bych mu vytknul.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*100 (A)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Je samozřejmě škoda, že se nepodařilo prolomit šifrování ani identifikovat autora viru. To však ani nelze po studentovi požadovat, protože v tomtéž selhávají i profesionální týmy antivirových společností. V tomto srovnání si naopak student vedl velmi dobře a i přes nedostatky zejména v jazykové oblasti si zaslouží, aby jeho práce byla hodnocena stupněm A, protože jde daleko nad rámec toho, co by diplomová práce měla demonstrovat.

Podpis vedoucího práce: