Posudek práce

předložené na Přírodovědecké fakultě JU

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

Autor:	**Bc. Martin Kunc**
Název práce:	**Dynamická analýza malware s cílem získávání indikátorů kompromitace a jejich následném využití**
Studijní program a obor:	Aplikovaná informatika
Rok odevzdání:	2019

Jméno a tituly vedoucího:	**Mgr. Jiří Pech, Ph.D.**
Pracoviště:	UAI
Kontaktní e-mail:	pechj@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 oponenta:

Autor si zvolil velmi zajímavé téma práce s obrovským potenciálem. Bohužel na práci je znát, že její sepsání autor oddaloval a pak jí sepisoval narychlo. Informace jsou uvedené roztříštěně a je třeba pozorné čtení, aby čtenář nepřišel o podstatné informace.

Například autor popisuje v úvodní části, že práci zpracovával výhradně na jednodeskovém počítači RaspBerry Pi. Protože však nemohl otestovat množství vzorků, kvůli architektuře jeho procesoru, později uvádí, že použil i klasické PC. Zde bohužel nezmiňuje (anebo je to opět zmíněno někde jinde), použitý operační systém.

Zcela chaotické se jeví tabulky na stranách 11 a 12. Jednak není jasné, jak autor přišel na čísla, kterými hodnotí jednotlivé možnosti a za druhé autor zdá se nedělá rozdíly mezi různými způsoby vyhodnocení (best-case a worst-case).

Dále je v práci zmíněno, že se jedná o více než rok staré vzorky, které budou podrobeny dalšímu zkoumání. Zde se samozřejmě nabízí otázka, zda takovýto výzkum je aktuální a má tudíž smysl.

Rovněž rozsah práce je pro tento typ práce poněkud nedostatečný.

Přes uvedené výtky, práci **doporučuji k obhajobě** a hodnotím stupněm **dobře**.

Případné otázky při obhajobě a náměty do diskuze:

1) Byly v mezidobí mezi sepsáním práce a touto obhajobou s daty prováděny nějaké další testy, jak je v práci popsáno?
2) Autor uvádí, že vše kontroloval a ověřoval kryptografickým otiskem pomocí programu sha256sum. Jak bylo zajištěno, že sám tento program nebyl kompromitován?
3) Jaký byl použit operační systém na klasickém PC?

Práci
☑ doporučuji
☐ nedoporučuji
uznat jako diplomovou.

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

Místo, datum a podpis oponenta: Pecl

V Českých Budějovicích 7. 5. 2019

Posudek práce

předložené na Přírodovědecké fakultě JU

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

Autor/ka: Bc. Martin Kunc
Název práce: Dynamická analýza malware s cílem získávání indikátorů kompromitace a jejich následném využití
Studijní program a obor: Aplikovaná informatika
Rok odevzdání: 2019
Jméno a tituly ~~vedoucího~~/oponenta: Ing. Jan Fesl, Ph.D.
Pracoviště: UAI PRF JU
Kontaktní e-mail: fesl@post.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/oponenta:

Předložená práce Bc. Martina Kunce obsahuje velmi zajímavou problematiku identifikace malwaru, která je v praxi velmi prospěšná. Z práce je patrná autorova zainteresovanost do problematiky a lze kladně hodnotit i to, že autor má o problematice všeobecný přehled.

Zásadní slabinou práce je její koncept, který je v dnešní době již překonaný, tzn. existuje již řada systémů, které konkrétní druhy malwaru identifikují na základě algoritmů opírající se o umělou inteligenci dynamicky přímo z dat získaných reportováním provozu ze směrovačů viz např. https://www.stratosphereips.org/.

V práci je ovšem i několik autorových domněnek, které dle mého názoru nejsou zcela technicky korektní – a sice, že malware je schopen automaticky rozpoznat virtuální prostředí (lze potlačit), virtualizer VirtualBox podporuje již od verze 6.06 USB 2.0/3.0. QEMU lze samozřejmě provozovat i pod virtuálním počítačem a tím pádem autorova primární výhoda u použití „nativního PC v podobě RaspBerry Pi" zcela odpadá.

Osobně se domnívám, že autor měl problematiku univerzálně vyřešit čistě virtualizačním způsobem a prozkoumat možnosti jejího přizpůsobení pro znemožnění její detekce. Autor například vůbec nezmínil použití "kontejnerové virtualizační technologie", která by v prostředí OS Linux nemusela zmíněným neduhem detekovatelnosti trpět vůbec – více info lze nalézt na https://remnux.org/docs/containers/malware-analysis/.

Práce je napsána srozumitelně, má logickou stavbu a je možné dle této provedené experimenty zopakovat. Úroveň zpracování je na úrovni magisterské práce diskutabilní, student pouze propojil existující nástroje (tcpdump, ssdeep, scp atd..) na úrovni skriptů ve funkční celek, což mi u tohoto druhu práce přijde za obtížně akceptovatelné. Práce je poměrně i krátká obsahově, méně než cca. 25 stran textu včetně obrázků, bereme-li v potaz pouze vlastní text bez příloh.

Nicméně, pokud srovnám předchozí práci studenta, která trpěla řadou dalších nedostatků, je zjevné, že autor udělal určitý pokrok vpřed. Autor sám je člověkem, který řadu let aktivně působí v CSIRT týmu sdružení CZNIC a o danou problematiku se dle mé osobní zkušenosti dlouhodobě zajímá.

Případné otázky při obhajobě a náměty do diskuze:

Práci
☑ doporučuji
☐ nedoporučuji
uznat jako diplomovou/~~bakalářskou~~.

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

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