Posudek oponenta bakalářské práce

Student: Vojtáš Samuel
Téma: Metody analýzy a detekce ransomwaru (id 24307)
Oponent: Kolář Dušan, doc. Dr. Ing., UIFS FIT VUT

1. **Náročnost zadání** — **obtížnější zadání**
   Zadání považuji za obtížnější, neboť vyžaduje získání dodatečných znalostí a dovedností z oblasti reverzního inženýrství, malware a kryptografie.
2. **Splnění požadavků zadání** — **zadání splněno**
   Zadání bylo splněno ve všech bodech.
3. **Rozsah technické zprávy** — **je v obvyklém rozmezí**
   Zpráva je v obvyklém rozmezí a to ve všech svých částech.
4. **Prezentační úroveň předložené práce** — **90 b. (A)**
   Jednotlivé části na sebe pěkně navazují, text je poměrně dobře čitelný, i když by si místy zasloužil hlubší popis a vysvětlení, tu a tam sklouzává k jisté schematičnosti. Trošku mi chybí RetDec v přehledu dekompilátorů.
5. **Formální úprava technické zprávy** — **90 b. (A)**
   Po formální stránce se dá vytknout jen pár drobností, např. strana 24 a přetečený řádek, nebo to, že je někde "kontrolný server", on asi nebude nic kontrolovat, on to bude řídit.
6. **Práce s literaturou** — **99 b. (A)**
   Podle mě dobrá.
7. **Realizační výstup** — **99 b. (A)**
   Výstupem primárně není programové dílo. Výstupem jsou pravidla pro detekci malware prostřednictvím programu YARA, která byla definována a prakticky se používají. Dále byl upraven program pro dešifrování souborů pro další rodinu malware. Osobně to u takovéhoto typu práce považuji za dostatečný a povedený výstup.
8. **Využitelnost výsledků**
   Výsledky jsou prakticky nasazeny pro detekci malware a pro případ jedné rodiny ransomware dokonce pro dešifrování zašifrovaných dat.
9. **Otázky k obhajobě**
   -
10. **Souhrnné hodnocení** — **90 b. výborně (A)**
    Práce vyžadovala od studenta nastudovat nové a pro něj neznámé techniky, postupy. Získat nové vědomosti. To vše nad rámec běžného Bc. studia. Analyzoval chování několika vzorků ransomware a vytvořil pravidla pro detekci. Upravil nástroj pro dešifrování dat pro další rodinu ransomware. Podle mého názoru nadstandardní práce.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 31. května 2022

Kolář Dušan, doc. Dr. Ing.
oponent