

Posudek oponenta diplomové práce

Student: Šrubař Michal, Bc.

Téma: Analýza síťové komunikace Ransomware (id 20204)

Oponent: Grégr Matěj, Ing., Ph.D., UIFS FIT VUT

1. **Náročnost zadání** obtížnější zadání
Práce se zabývá analýzou ransomware, zadání považuji svým rozsahem za obtížnější.
2. **Splnění požadavků zadání** zadání splněno
3. **Rozsah technické zprávy** je v obvyklém rozmezí
4. **Prezentační úroveň předložené práce** 80 b. (B)
Prezentační úroveň technické zprávy je kvalitní. Kapitoly jsou vhodně členěné a dobře na sebe navazují. Práce je pro čtenáře pochopitelná. Výtku mám zejména ke grafům (4.1, 4.2), na kterých není popsána osa y, takže jsou grafy obtížněji interpretovatelné.
5. **Formální úprava technické zprávy** 90 b. (A)
Jazykově i typograficky je práce kvalitní. Občas lze nalézt překlep, ale obecně je práce vcelku bez chyb.
6. **Práce s literaturou** 80 b. (B)
V práci jsou použité citace dle zvyklosti a citační normy. V textu jsou citace správně použity. Výtku mám pouze k tomu, že u některých citací (např. [2], [6]) bych ocenil i odkaz na url.
7. **Realizační výstup** 90 b. (A)
Praktická část práce spočívala v testování a zkoumání provozu malware. Bylo připraveno testovací prostředí a analyzováno množství různého malware. Výsledkem jsou detektory, které byly testovány jak vůči ransomware provozu, tak i v běžné síťové komunikaci.
8. **Využitelnost výsledků**
Informace získané analýzou dat mohou být dále použity pro zkoumání síťového provozu ransomware programů.
9. **Otázky k obhajobě**
-
10. **Souhrnné hodnocení** 90 b. výborně (A)
Práce se zabývá analýzou ransomware. Díky rozboru ransomware WCRY je obsahově velmi aktuální. Část práce se podařilo publikovat jako analýzu na serveru zive.cz. Jak textovou část, tak realizační výstup hodnotím jako kvalitní. Celkově práci považuji za výbornou (A).

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

V Brně dne: 2. června 2017

.....
podpis