Review of Master's Thesis

Student: Holop Patrik, Bc.
Title: Real-Time Detection of Malware Campaigns (id 23731)
Reviewer: Polčák Libor, Ing., Ph.D., DIFS FIT BUT

1. **Assignment complexity** — **more demanding assignment**
   Úspěšné zvládnutí práce zahrnovalo seznámení se s interními systémy a procesy Avastu, možnostmi detekce kampaní, zpracováním velkého množství dat, tvorbou webového GUI a důkladného testování.
2. **Completeness of assignment requirements** — **assignment fulfilled with enhancements**
   Zadání bylo splněno. Nad rámec zadání došlo k vyhodnocení systému detekce vůči externím zdrojům, které mělo vliv na doladění detekčních mechanismů. Podle informací v kapitole 7 byl systém testován již v lednu a únoru 2021.
3. **Length of technical report** — **in usual extent**
   Podle http://standardpages.herokuapp.com/standardpages/ má práce 102 normostran.
4. **Presentation level of technical report** — **90 p. (A)**
   Práce byla psaná pochopitelně a přestože se jedná o práci založenou na přístupech konkrétní společnosti, byly podstatné rysy dobře vysvětleny. Výhrady mám k sekci 3.6, která pro mě nebyla napsaná pochopitelně. Pro název kapitoly 5 bych volil pojmenování odkazující se na návrh. Občas se objevil příliš dlouhý odstavec.
5. **Formal aspects of technical report** — **95 p. (A)**
   Práce je psaná velmi pěkným anglickým jazykem, jen občas jsem narazil na drobnost, kterou bych formuloval jinak. Některé pojmy byly použity v hovorovém tvaru (např. legit).

   Nenarazil jsem na žádný typografický problém.
6. **Literature usage** — **100 p. (A)**
   Práce obsahuje širokou škálu relevantních zdrojů.
7. **Implementation results** — **100 p. (A)**
   Zdrojové kódy jsou rozsáhlé, dělené do modulů, komentované a působí velice přehledně. Práce obsahuje stovky testů. Student mně předvedl a okomentoval nasazení systému v rámci Avastu.
8. **Utilizability of results**
   Na základě mně předložených informací se práce jeví jako pro Avast použitelná (více v první otázce k obhajobě).
9. **Questions for defence**
   - V kapitole 7 zmiňujete kampaně popsané externími zdroji. Většina záznamů je z období ledna až března 2021. Je systém Avastem používán i v dalších měsících?
   - Jaké množství dat váš systém zpracovával? Byla to všechna podporovaná data, která má Avast k dispozici?
10. **Total assessment** — **99 p. excellent (A)**
    Pan Holop vytvořil vysoce nadstandardní práci. Zdrojový kód vypadá velmi kvalitně, detekce byla dlouhodobě testována. Doporučuji hodnotit práci jako výbornou (A).

In Brno 1 June 2021

Polčák Libor, Ing., Ph.D.
reviewer