Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK VEDOUCÍHO BAKALÁŘSKÉ PRÁCE

Jméno studenta: Radek Netolický

Název práce: Moderní techniky analýzy malware

Autor posudku: Ing. Tomáš Svoboda, Ph.D.

Cíl práce: Cílem práce je vytvoření dílčích úloh statické a dynamické analýzy malware dle předem definovaných use-case

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)					
	A	**B**	**C**	**D**	**E**	**F**
Práce svým zaměřením odpovídá studovanému oboru	☒	☐	☐	☐	☐	☐
Vymezení cíle a jeho naplnění	☐	☒	☐	☐	☐	☐
Zpracování teoretických aspektů tématu	☐	☒	☐	☐	☐	☐
Zpracování praktických aspektů tématu	☐	☒	☐	☐	☐	☐
Adekvátnost použitých metod, způsob jejich použití	☐	☒	☐	☐	☐	☐
Hloubka a správnost provedené analýzy	☐	☒	☐	☐	☐	☐
Práce s literaturou	☐	☒	☐	☐	☐	☐
Logická stavba a členění práce	☐	☒	☐	☐	☐	☐
Jazyková a terminologická úroveň	☐	☒	☐	☐	☐	☐
Formální úprava a náležitosti práce	☐	☒	☐	☐	☐	☐
Vlastní přínos studenta	☐	☒	☐	☐	☐	☐
Využitelnost výsledků práce v teorii (v praxi)	☐	☒	☐	☐	☐	☐

Vyjádření k výsledku anti-plagiátorské kontroly

Antiplagiátorská kontrola eVSKP identifikovala celkovou podobnost: 6%. Jedná se převážně o shodu při používání všeobecně známých pojmů z oblasti informační a kybernetické bezpečnosti, které jsou korektně citovány.

Dílčí připomínky a náměty:

Vedoucí práce nemá zásadní připomínky k předložené práci.

Celkové posouzení práce a zdůvodnění výsledné známky:

Bakalářská práce se zabývá principy a praktickými technikami analýzy malware, což je oblast, která je velice aktuální vzhledem k nárůstu kybernetických útoků souvisejících s využitím malware.
V teoretické části práce autor nejprve představuje základní pojmy a historii zákona o kybernetické bezpečnosti včetně CIA moelu a Parkerian hexad modelu pro zajištění důvěrnosti, dostupnosti a integrity dat. Dále se autor zaměřuje na představení typů malware a popis jednotlivch typů, resp. rozdílů mezi jednotlivými typy malware. Stěžejní části je představení technik analýzy malware. Tytot techniky – statickou a dynamickou analýzu popisuje autor v kapitole 3.5 na odpovídající úrovni.
V praktické části práce autor na vzorku malware provádí jeho statickou a dynamickou analýzu. Je

škoda, že autor využil vzorek malware volně dostupný z internetu a nevytvořil si vlastní vzorek. Nebylo tak možné zcela potvrdit či vyvrátit pravdivost získaných informací o malware prostřednictvím statické a dynamické analýzy na vzorku staženém z internetu. Autor používá sadu nástrojů pro statickou a dynamickou analýzu (hashmyfiles, VirusTotal apod.), které jsou dle best-practise využitelné v této oblasti. Zároveň není zcela jasné, z jakého důvodu, resp. na základě jakých kritérií se autor rozhodl využít právě vybranou sadu nástrojů pro statickou a dynamickou analýzu malware, které autor používá. Bakalářská práce splňuje požadavky kladné na bakalářskou práci a doporučuji ji k obhajobě.

Otázky k obhajobě:

Představte kritéria na základě kterých jste vybral konkrétní nástroje pro statickou a dynamickou analýzu malware (hashmyfiles, virustotal, strings, wireshark apod.)?

Práci doporučuji k obhajobě.

Navržená výsledná známka: B

V Hradci Králové**, dne 3. května 2024**

podpis