Fakulta informatiky
Masarykova univerzita
Botanická 68a, 602 00 Brno

Posudek diplomové práce

Datum: 2. února 2014

Název:	Analysis of Malware Classification Schemes
Student:	Bc. Petr Nemček
Vedoucí:	Mgr. Vít Bukač
Oponent:	RNDr. Marek Kumpošt, Ph.D.

Zpráva:

Student se ve své práci zaměřil na srovnání vlastností různých formátů na popis Malware. V praktické části bylo úkolem navrhnout převodní nástroj mezi zvolenými formáty ve formě webové služby a vlastní implementace.

Práce je členěna do šesti kapitol – drtivá část práce je věnována popisu formátů, vlastní implementaci je věnováno pouze necelých 8 stran.

Při čtení práce mne jednak překvapila úroveň anglického jazyka a hned v zápětí i použití externích zdrojů. V kapitole 1 student čerpá výhradně ze zdroje [2], v kapitole 2 potom výhradně ze zdroje [3]. Při bližším prozkoumání za pomocí služby vyhledávání podobností v ISu bylo nalezeno netriviální množství přímo použitého textu z původního zdroje. Text v práci studenta ale není citován jako přímá citace (ačkoliv student zřejmě umí použít přímou citaci – viz strana 36).

Jeden příklad za všechny – doslovný přepis z knihy [3], na straně 13. „*A backdoor is a type of malware that provides an attacker with remote access to a victim's machine. Backdoors are the most commonly found type of malware, and they come in all shapes and sizes with a wide variety of capabilities. Backdoor code often implements a full set of capabilities, so when using a backdoor attackers typically don't need to download additional malware or code. Backdoors communicate over the Internet in numerous ways, but a common method is over port 80 using the HTTP protocol. HTTP is the most commonly used protocol for outgoing network,...*"

Vzhledem ke zjištěným skutečnostem jsem nevěnoval další pozornost praktické části.

Hodnocení:

Předloženou práci nedoporučuji k obhajobě a navrhuji hodnocení stupněm ***F***.

.....
Marek Kumpošt