ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Kouba** Jméno: **Dominik** Osobní číslo: **466040**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra počítačů**

Studijní program: **Otevřená informatika**

Specializace: **Kybernetická bezpečnost**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Analýza záznamů běhu malwaru pomocí hierarchického multi-instančního učení

Název diplomové práce anglicky:

Analyzing the execution of malware in a sandbox using hierarchical multiple instance learning

Pokyny pro vypracování:

The thesis aims to capture and analyze artifacts of malware execution in a protected environment and assess if these artifacts can be used to predict malware functionalities and capabilities.
1. Run several instances of CapeV2 sandbox and solve their orchestration for this experiment
2. Capture behavior of selected malware samples in CapeV2 sandbox and store results
3. Learn the hierarchical multiple instance learning framework (HMill)
4. Analyze captured data. Report basic statistics and choose appropriate features and hidden states for further modeling.
5. Using HMill, create models, and identify the artifacts corresponding to different malware behavior. Report results.
6. Investigate which parts of the CapeV2 log are important to different malware behavior.
7. Evaluate the results of the experiment.

Seznam doporučené literatury:

1. Jan Stiborek, Tomáš Pevný, and Martin Rehák. „Multiple instance learning for malware classification“ Expert Syst. Appl. 93, C (March 2018), 346–357, 2018.
2. Digit Oktavianto and Iqbal Muhardianto. „Cuckoo Malware Analysis“. Packt Publishing, 2013.
3. T. Pevný and P. Somol, „Using neural network formalism to solve multiple-instance problems,” in International Symposium on Neural Networks, pp. 135–142, Springer, 2017.
4. S. Mandlik, „Mapping the Internet — Modelling Entity Interactions in Complex Heterogeneous Networks (diploma thesis)“, 2020.
5. Wang C., Ding J., Guo T., Cui B. „A Malware Detection Method Based on Sandbox, Binary Instrumentation and Multidimensional Feature Extraction“. In: Barolli L., Xhafa F., Conesa J. (eds) Advances on Broad-Band Wireless Computing, Communication and Applications. BWCCA 2017. Lecture Notes on Data Engineering and Communications Technologies, vol 12. Springer, Cham., 2018.

Jméno a pracoviště vedoucí(ho) diplomové práce:

doc. Ing. Tomáš Pevný, Ph.D., centrum umělé inteligence FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **11.02.2021** Termín odevzdání diplomové práce: _____

Platnost zadání diplomové práce: **30.09.2022**

doc. Ing. Tomáš Pevný, Ph.D. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Mgr. Petr Páta, Ph.D. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

. _____ _____

Datum převzetí zadání Podpis studenta

