Дослідження шкідливого програмного забезпечення

Дмитро Юрчук, Іван Савка

Кафедра інформаційних технологій
Прикарпатський національний університет імені Василя Стефаника

2022 International Conference on Innovative Solutions in Software Engineering (ICISSE-2022)
Ivano-Frankivsk, Ukraine,
November 29-30, 2022

Актуальність роботи полягає в тому, що вірусне програмне забезпечення стрімко розвивається з кожним роком. Відповідно існує необхідність у вдосконаленні наявних та розробці нових засобів для розпізнавання шкідливого ПЗ, які в результаті можна використати при створенні нових антивірусних програм.

Основною метою даного дослідження є аналіз методів та засобів для розпізнавання шкідливого програмного забезпечення**.**

Об’єкт дослідження: шкідливе програмне забезпечення.

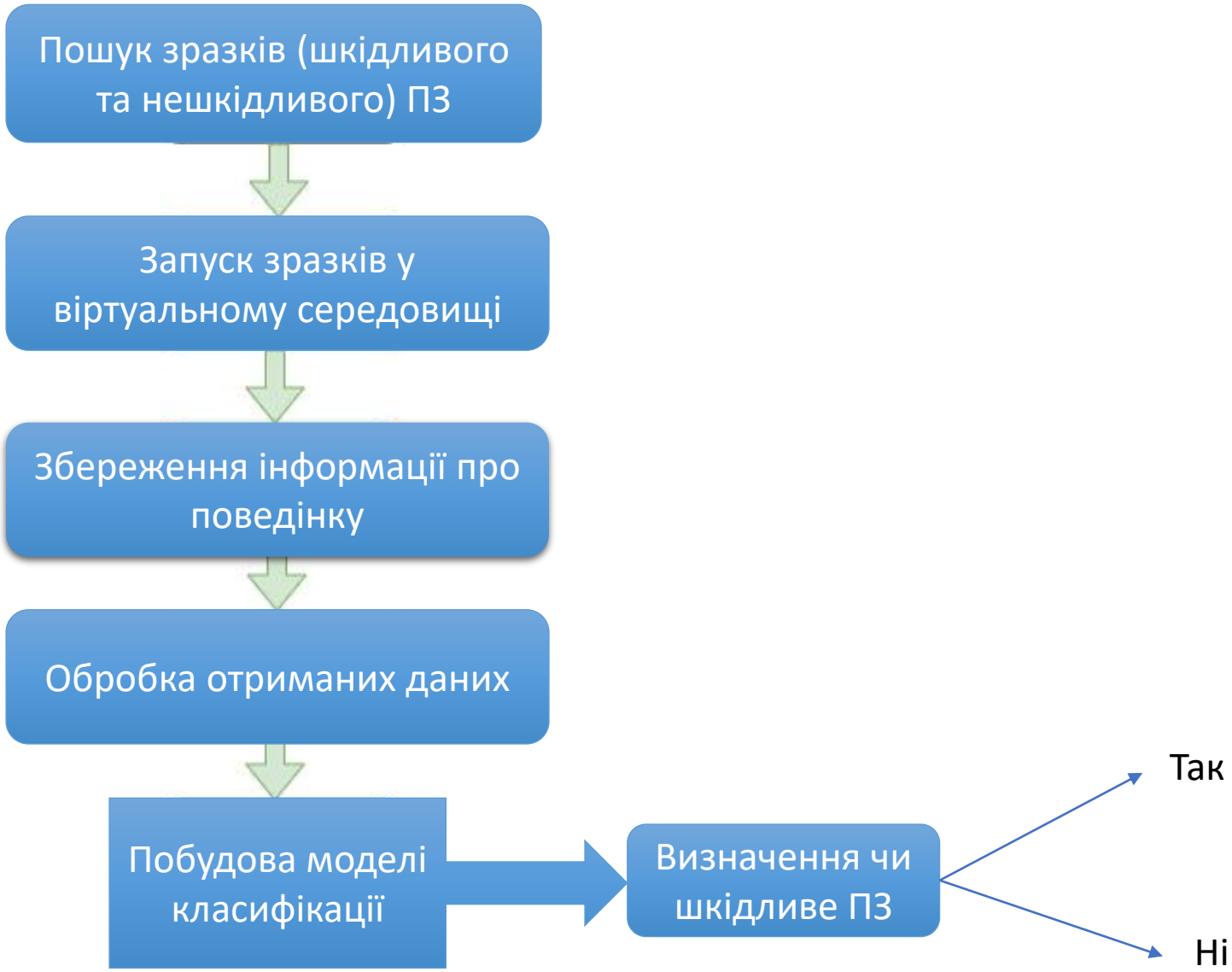
Пов’язані роботи

1) Md Jobair Hossain Faruk, Hossain Shahriar , Maria Valero , Farhat Lamia Barsha, Shahriar Sobhan Md Abdullah Khan, Michael Whitman, Alfredo Cuzzocreak , Dan Lo, Akond Rahman and Fan Wu, Eds., “Malware Detection and Prevention using Artificial Intelligence Techniques,” [Онлайн]. Доступно: https://arxiv.org/ftp/arxiv/papers/2206/2206.12770.pdf.
2) Zahra Bazrafshan, Hashem Hashemi, Seyed Mehdi Hazrati Fard, Ali Hamzeh, Eds., “A survey on heuristic malware detection techniques,” [Онлайн]. Доступно: https://www.researchgate.net/publication/260729684_A_survey_on_heuristic_malware_detection_techniques.
3) Malware analysis [Онлайн]. Доступно: https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis.
4) Daniel Gibert, Carles Mateu, Jordi Planes, Eds., “The rise of machine learning for detection and classification of malware: Research developments, trends and challenges,” in Journal of Network and Computer Applications, Mar. 2020. [Онлайн]. Доступно: https://www.researchgate.net/publication/338355873_The_rise_of_machine_learning_for_detection_and_classification_of_malware_Research_developments_trends_and_challenges.
5) Alfred Melvin, G. Jaspher W. Kathrine, “A Quest for Best: A Detailed Comparison Between Drakvuf-VMI-Based and Cuckoo Sandbox-Based Technique for Dynamic Malware Analysis” in “Intelligence in Big Data Technologies—Beyond the Hype,” J. Dinesh Peter, Steven L. Fernandes, Amir H. Alavi, Eds., Singapore, 2021, pp. 275-290.


Сигнатурний
Поведінковий
Евристичний
Методи виявлення шкідливого ПЗ


Статичний
Динамічний
Гібридний
Методи аналізу шкідливого ПЗ

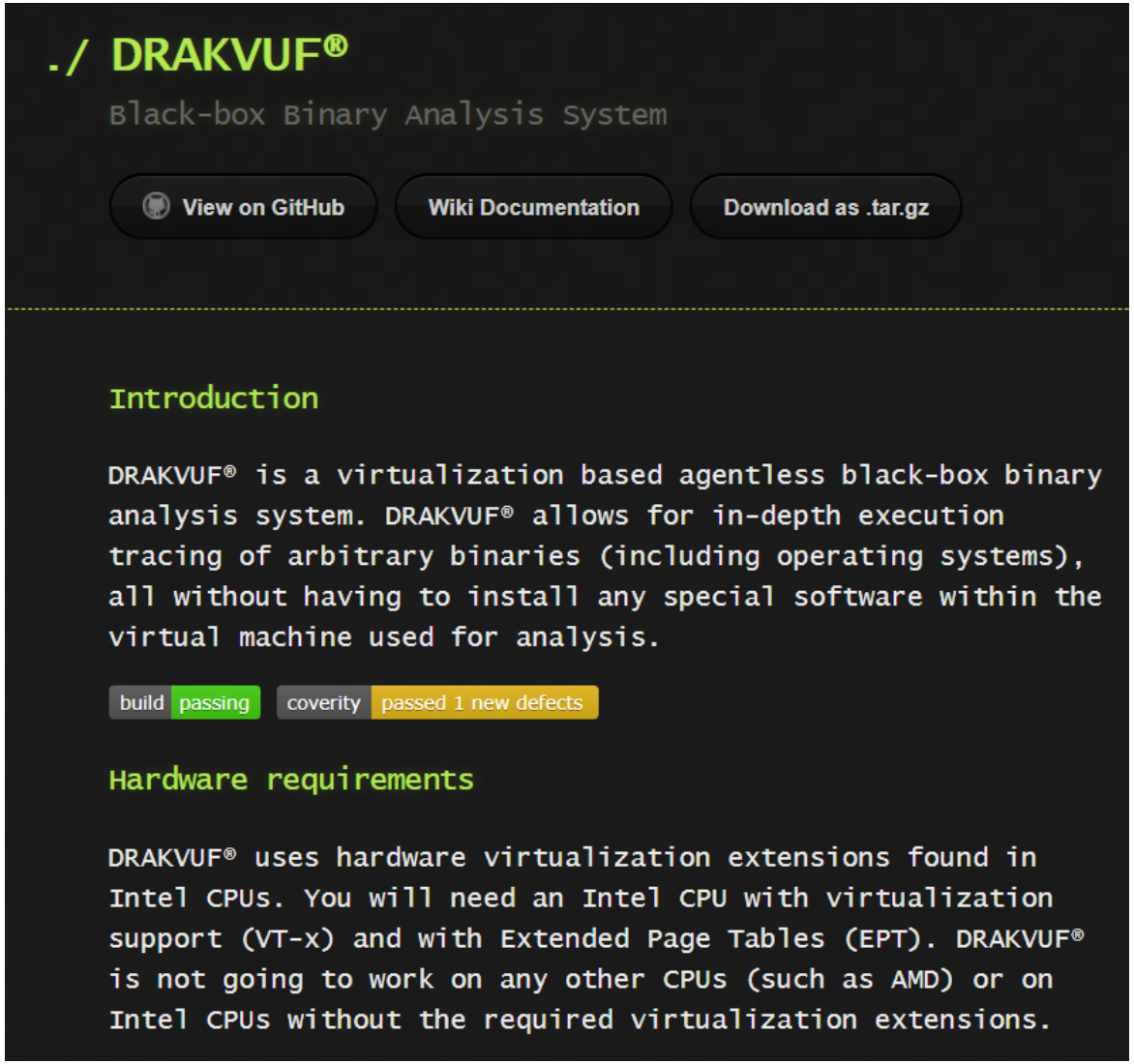
Схема визначення шкідливого ПЗ на основі динамічного аналізу



Cucko


cuckoo
Automated Malware Analysis
Home
Downloads
Partners
Docs
Blog
About Cuckoo
Discussion
What is Cuckoo?
Cuckoo Sandbox is the leading open source automated malware analysis system.
cuckoo
You can throw any suspicious file at it and in a matter of minutes Cuckoo will provide a detailed report outlining the behavior of the file when executed inside a realistic but isolated environment.
Malware is the swiss-army knife of cybercriminals and any other adversary to your corporation or organization.
Download Cuckoo Sandbox 2.0.7
Contribute to Cuckoo
More downloads
READ NOW:
Cuckoo Sandbox 2.0.7
Posted on June 19, 2019
Read this blogpost!

Drakvuf


./ DRAKVUF®
Black-box Binary Analysis System
View on GitHub
Wiki Documentation
Download as .tar.gz
Introduction
DRAKVUF® is a virtualization based agentless black-box binary analysis system. DRAKVUF® allows for in-depth execution tracing of arbitrary binaries (including operating systems), all without having to install any special software within the virtual machine used for analysis.
build passing
coverity passed 1 new defects
Hardware requirements
DRAKVUF® uses hardware virtualization extensions found in Intel CPUs. You will need an Intel CPU with virtualization support (VT-x) and with Extended Page Tables (EPT). DRAKVUF® is not going to work on any other CPUs (such as AMD) or on Intel CPUs without the required virtualization extensions.

Результати дослідження

- розгляд методів розпізнавання вірусного ПЗ;
- визначення можливих методів для аналізу шкідливого ПЗ;
- опис методики динамічного аналізу вірусів та необхідних засобів для цього.

Висновки

- Безпека інформації є важливою, оскільки будь-які вірусні атаки несуть за собою в першу чергу економічні збитки для будь-якої організації.
- Аналіз вмісту програм, оновлення наборів даних шкідливого ПЗ і використання методів штучного інтелекту дозволяє виявляти нові загрози, розробляти та впроваджувати ефективні заходи для забезпечення потрібного рівня кіберзахисту.

Дякую за увагу!