УДК 004.056.5

Д.В. Яцюк
В. В. Гуменюк
В.М. Білоус

ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ ПРОТИДІЇ АНТИВІРУСНОМУ ВИЯВЛЕННЮ У ШКІДЛИВОМУ ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ

Вінницький національний технічний університет

Анотація

Об’єктом дослідження є методи протидії антивірусному виявленню, що застосовуються у шкідливому програмному забезпеченні. У межах роботи проаналізовано сучасні підходи до обходу сигнатурного, евристичного та поведінкового контролю, зокрема обфускацію коду, пакування, антиналагоджувальні прийоми, маніпуляції з таблицею імпорту та середовищно-залежні механізми виконання. Запропоновано алгоритм багаторівневої оцінки ознак протидії антивірусному виявленню, який поєднує статичний, поведінковий і середовищний аналіз та враховує комбінований ефект кількох технік. Практичне значення одержаних результатів полягає у можливості використання запропонованого підходу як логічної основи для систем раннього виявлення підозрілих зразків і навчальних стендів з кібербезпеки.

Ключові слова: кібербезпека, інформаційна безпека, шкідливе програмне забезпечення, антивірусний захист, виявлення загроз, обфускація коду.

Abstract

The object of the study is the set of methods used by malicious software to resist antivirus detection. The paper analyzes current approaches to bypassing signature-based, heuristic, and behavioral controls, including code obfuscation, packing, anti-debugging techniques, import table manipulation, and environment-dependent execution mechanisms. A multi-level algorithm for assessing indicators of resistance to antivirus detection is proposed; it combines static, behavioral, and environmental analysis while taking into account the cumulative effect of multiple techniques. The practical value of the obtained results lies in the possibility of using the proposed approach as a logical basis for early warning systems for suspicious samples and cybersecurity training environments.

Keywords: cybersecurity, information security, malware, antivirus protection, threat detection, code obfuscation.

Вступ

Проблема захисту комп’ютерних систем від шкідливого програмного забезпечення залишається однією з найактуальніших у галузі кібербезпеки. Із розвитком засобів захисту одночасно ускладнюються і методи їх обходу, що знижує ефективність традиційних сигнатурних підходів і підвищує роль поведінкового аналізу.

Сучасні шкідливі програми дедалі частіше поєднують декілька технік протидії антивірусному виявленню, орієнтованих не лише на приховування коду, а й на ускладнення динамічного аналізу, перевірку характеристик середовища та зрив дослідження в ізольованих умовах. Метою роботи є дослідження сучасних методів протидії антивірусному виявленню у шкідливому програмному забезпеченні та побудова алгоритму багаторівневої оцінки ознак застосування таких методів.

Результати дослідження

Проведений аналіз літературних джерел показав, що в сучасних засобах обходу антивірусного контролю домінує комбіноване застосування кількох технік. У дослідженні Barchuk та Volkov [1] узагальнено базові підходи до обходу антивірусного захисту, серед яких виділено обфускацію, пакування, завантажувачі, антиналагоджувальні прийоми та маніпуляції зі структурою виконуваних файлів. Автори

підкреслюють, що найбільшу складність для засобів захисту становить не окреме використання цих прийомів, а їх комбінування в межах одного зразка шкідливого програмного забезпечення.

Результати Samociuk [2] демонструють, що ефективність окремих інструментів протидії антивірусному виявленню залежить від актуальності їх реалізації, частоти оновлень та здатності модифікувати корисне навантаження без втрати функціональності. Це підтверджує динамічний характер протистояння між шкідливим програмним забезпеченням і засобами захисту.

У роботі Jin et al. [3] показано, що автоматизована генерація варіантів шкідливого програмного забезпечення на основі генетичних алгоритмів дозволяє суттєво підвищити здатність зразків протидіяти антивірусному виявленню. Отже, для адекватної оцінки загрози доцільно враховувати не окрему ознаку, а сукупність статичних, поведінкових і середовищних індикаторів.

Огляд Kaur et al. [4] засвідчує, що сучасні рішення захисту дедалі більше спираються на поведінкову аналітику, машинне навчання та кореляцію подій на різних рівнях інфраструктури. Водночас у роботі Padhy et al. [5] продемонстровано, що перевірки наявності налагоджувача, середовищно-залежні механізми виконання та ускладнення статичного аналізу залишаються ефективними засобами протидії традиційним механізмам виявлення.

На основі проведеного аналізу запропоновано алгоритм багаторівневої оцінки ознак протидії антивірусному виявленню, який передбачає послідовне врахування трьох груп показників: статичних, поведінкових і середовищних. У межах статичного аналізу оцінюються ентропія секцій, ознаки пакування, аномалії таблиці імпорту, нетипова структура PE-файлу та обфускація рядків. Під час поведінкового аналізу в контрольованому середовищі фіксуються ознаки саморозпакування, затримки виконання, ін'єкції в процеси, підозрілі виклики API, модифікації реєстру та мережева активність. Середовищний рівень включає перевірки наявності віртуалізації, налагоджувача, прив'язки до апаратних параметрів і аномалії TLS-callback.

Для кількісного подання результату використано інтегральний показник ризику протидії антивірусному виявленню:

$$R = w_1 S + w_2 D + w_3 E + kC$$

де S - оцінка статичних ознак, D - оцінка поведінкових ознак, E - оцінка середовищних індикаторів, C - коефіцієнт комбінованого застосування технік протидії, w_1, w_2, w_3, k - вагові коефіцієнти моделі.

На відміну від підходів, що розглядають окремі техніки ізольовано, запропонований алгоритм дозволяє оцінювати їх сукупний вплив на зниження ймовірності антивірусного виявлення.

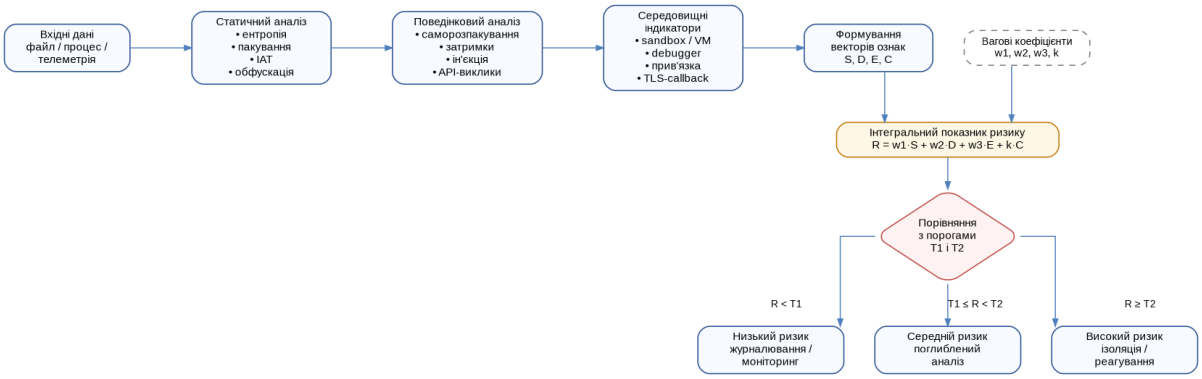

Рис. 1. Функціональна схема багаторівневої оцінки ознак протидії антивірусному виявленню

Практичне значення запропонованого алгоритму полягає в можливості його використання як логічної основи для систем раннього виявлення підозрілих зразків, аналітичних модулів захисту кінцевих точок або навчальних стендів із кібербезпеки.

Висновки

У результаті дослідження встановлено, що сучасне шкідливе програмне забезпечення використовує складні багатокомпонентні методи протидії антивірусному виявленню, які поєднують обфускацію, пакування, антиналагодження, середовищну прив'язку та інші засоби протидії аналізу. Окремий розгляд таких технік є недостатнім для оцінки реального рівня загрози.

Наукова новизна роботи полягає у побудові алгоритму багаторівневої оцінки ознак протидії антивірусному виявленню, який інтегрує статичний, поведінковий і середовищний аналіз у єдину схему оцінювання та враховує комбінований вплив кількох технік ухилення.

Практичне значення отриманих результатів полягає в можливості використання запропонованого підходу під час розроблення аналітичних модулів виявлення підозрілих зразків, навчальних стендів і моделей оцінювання ризику в системах кіберзахисту. Подальші дослідження доцільно спрямувати на уточнення вагових коефіцієнтів алгоритму та його апробацію на вибірках реальних і модифікованих зразків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Barchuk B., Volkov K. Antivirus evasion techniques in modern malware. World Journal of Advanced Research and Reviews. 2025. DOI: https://doi.org/10.30574/wjarr.2025.26.2.1966.
2. Samociuk D. Antivirus Evasion Methods in Modern Operating Systems. Applied Sciences. 2023. DOI: https://doi.org/10.3390/app13085083.
3. Jin B., Choi J., Hong J. B., Kim H. On the Effectiveness of Perturbations in Generating Evasive Malware Variants. IEEE Access. 2023. DOI: https://doi.org/10.1109/ACCESS.2023.3262265.
4. Kaur H. et al. Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review. E3S Web of Conferences. 2024. DOI: https://doi.org/10.1051/e3sconf/202455601006.
5. Padhy S. T., Shanthi P. B., Bijur G., Hemalatha S. A Threat-Informed Approach to Malware Evasion Using DRM and TLS Callbacks. IEEE Access. 2025. DOI: https://doi.org/10.1109/ACCESS.2025.3605020.

Яцюк Денис Володимирович – студент групи 3КІТС-23б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: denis.yatsuk22@gmail.com.

Гуменюк Вячеслав Володимирович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: hvv@vntu.edu.ua.

Науковий керівник: Білоус Віталій Михайлович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: vitalii.bilous@vntu.edu.ua.

Yatsiuk Denys Volodymyrovych – student of group 3KITS-23b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: denis.yatsuk22@gmail.com.

Humeniuk Viacheslav Volodymyrovych – Assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: hvv@vntu.edu.ua.

Scientific supervisor: Bilous Vitalii Mykhailovych – Assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: vitalii.bilous@vntu.edu.ua.