УДК 004.056.5

А.В. Семенюк

ПРОБЛЕМАТИКА ВИЯВЛЕННЯ ШКІДЛИВИХ ПРОГРАМ В КОМП'ЮТЕРНИХ СИСТЕМАХ

Вінницький національний технічний університет

Анотація

У сучасному цифровому світі зростає загроза від шкідливих програм, які можуть пошкодити комп'ютерні системи та викрасти особисту інформацію користувачів. Ця стаття розглядає проблематику виявлення шкідливих програм в комп'ютерних системах та пропонує стратегії й методи боротьби з ними. Також здійснюється аналіз різноманітних типів шкідливих програм, їх методів обходу захисту. Висвітлено тему використання новітніх технологій, таких як машинне навчання та штучний інтелект, для виявлення та нейтралізації подібних загроз.

Ключові слова: шкідливі програми, комп'ютерні системи, кібербезпека, виявлення, антивірусні програми, машинне навчання, штучний інтелект.

Abstract

In today's digital world, there is a growing threat of malware that can damage computer systems and steal users' personal information. This article examines the problem of detecting malicious programs in computer systems and offers strategies and methods for combating them. Analysis of various types of malicious programs and their methods of bypassing protection is also carried out. The topic of using the latest technologies, such as machine learning and artificial intelligence, to detect and neutralize such threats is covered.

Key words: malware, computer systems, cyber security, detection, antivirus, machine learning, artificial intelligence.

Вступ

У сучасному світі комп'ютери і мережа Інтернет стали невід'ємною частиною нашого повсякденного життя. Ми використовуємо їх для комунікації, розваг, роботи, навчання тощо. Однак разом із зростанням кількості комп'ютерних систем, що використовуються – пропорційно збільшується і загроза від шкідливих програм, які можуть завдати шкоди цим системам, викрасти певну особисту інформацію та завдати шкоди даним, що там зберігаються.

Метою дослідження є аналіз та вивчення проблематики виявлення шкідливих програм в комп'ютерних системах з метою розробки ефективних стратегій та методів боротьби з цими загрозами для забезпечення безпеки та захисту користувачів та їхніх даних.

Об'єктом дослідження є процес виявлення та аналізу шкідливих програм в комп'ютерних системах. Це включає в себе як традиційні методи виявлення вірусів та шкідливого програмного забезпечення, так і нові підходи, що базуються на машинному навчанні та штучному інтелекті.

Предметом дослідження є механізми та технології, що використовуються для виявлення та аналізу шкідливих програм, а також фактори, що впливають на ефективність цих методів.

Головною задачею є розробка інноваційних підходів та методів виявлення шкідливих програм в комп'ютерних системах, які б дозволили ефективно впоратися з постійною загрозою кібербезпеки користувача. Це включає в себе аналіз сучасних технологій, їхніх переваг та недоліків, а також впровадження нових підходів, що базуються на передових методах машинного навчання та штучного інтелекту.

Проблематика виявлення шкідливих програм

Проблема виявлення шкідливих програм в комп'ютерних системах стає все більш актуальною, оскільки кількість таких програм постійно зростає, а методи зламу та проникнення стають більш досконалими. Виявлення шкідливих програм важливо для забезпечення безпеки і захисту комп'ютерних систем та особистих даних користувачів. Однак це завдання не завжди є легким через різноманітність шкідливих програм та їхні техніки обходу захисту.

Однією з основних проблем виявлення шкідливих програм є їхня постійна еволюція та зміна. Розробники шкідливих програм постійно вдосконалюють свої методи, щоб уникнути виявлення та нейтралізації захисними механізмами. Вони використовують різні техніки, такі як шифрування коду, поліморфізм, використання нульових днів та інші для того, щоб уникнути виявлення антивірусними програмами.

Ще однією проблемою є поява нових видів шкідливих програм, які можуть проникати в систему без виявлення традиційними методами. Наприклад, адаптивні програми, які можуть змінювати свою поведінку в залежності від середовища, або програми з використанням штучного інтелекту для аналізу та обходу систем захисту. Ці нові підходи ускладнюють завдання виявлення та боротьби зі шкідливими програмами.

Іншою проблемою є великий обсяг даних, який потрібно аналізувати для виявлення шкідливих програм[4]. Впоратись з аналізом великої кількісті файлів, мережевого трафіку та інших джерел інформації в стислі терміни – важка задача. Аналітичні механізми зі збору і обробки даних повинні використовувати ефективні алгоритми та інструменти для виявлення підозрілої активності. Та навіть за умови їх використання – це може бути досить затратною процедурою, особливо у розрізі великих корпоративних мереж чи хмарних платформ.

Також слід враховувати соціальні і психологічні аспекти, які впливають на виявлення шкідливих програм. Наприклад, соціальна інженерія, яка використовується шкідливими програмами для виклику у користувачів певних дій, таких як натискання на посилання або відкриття вірусних додатків. Часто люди стають слабкими ланками у цьому процесі через недостатню освіченість щодо безпеки в Інтернеті.

Інноваційні підходи та методи виявлення шкідливих програм

Вирішення проблеми виявлення шкідливих програм у комп'ютерних системах є надзвичайно важливим завданням, що стає все більш складним у зв'язку з постійним розвитком технологій та зростанням кількості та складності шкідливих програм. Нижче представлені основні й додаткові стратегії та підходи до вирішення цієї проблеми:

- розвиток технологій кібераналізу – розробка нових інструментів та методів аналізу великих обсягів даних для виявлення незвичайної або підозрілої активності. Використання технологій «Big Data» та «Data Mining» дозволяє виявляти патерни та залежності, що можуть бути пов'язані із шкідливою діяльністю;

- системи виявлення вразливостей – розробка та впровадження систем, які автоматично виявляють вразливості у програмному забезпеченні та операційних системах. Це допомагає уникнути використання зловмисниками вразливостей для впровадження шкідливих програм;

- просунуті алгоритми обробки даних – використання технік машинного навчання[2] та штучного інтелекту для виявлення аномальної поведінки програм. Це включає в себе аналіз динамічних властивостей програм, таких як системні виклики та мережева активність, що є необхідним для виявлення відхилень від типової поведінки;

- глобальна кооперація – залучення міжнародних організацій, компаній та урядових установ для обміну інформацією про виявлені загрози та застосовані методи їхнього виявлення. Це дозволяє

ефективніше виявляти та нейтралізувати шкідливі програми, які можуть атакувати системи у різних частинах світу;

- неперервне навчання та адаптація – розробка систем, які постійно навчаються на основі нових даних та інформації про вже виявлені загрози. Це дозволяє створювати більш ефективні та адаптивні методи виявлення шкідливих програм, які можуть пристосовуватися до високо динамічних змін у загрозах та технологіях.

В цілому, вирішення проблеми виявлення шкідливих програм в комп'ютерних системах вимагає комплексного підходу та поєднання різноманітних стратегій та технологій. Тільки такий підхід дозволить забезпечити ефективний захист від кіберзагроз, що мають доволі динамічний розвиток та вдосконалення.

Зрештою, важливою складовою боротьби з шкідливими програмами є освіта користувачів та дотримання певних правил інформаційної гігієни. Інформування про загрози в Інтернеті та навчання базовим принципам кібербезпеки може допомогти уникнути багатьох атак. Підвищення свідомості користувачів про потенційні небезпеки та методи їхнього запобігання може допомогти зменшити кількість успішних атак шкідливих програм.

Висновки

У підсумку, проблема виявлення шкідливих програм в комп'ютерних системах є складною та доволі динамічною. Ця стаття демонструє потенційну загрозу, яку становлять шкідливі програми для безпеки користувачів у цифровому середовищі, а також вказує на важливість розробки та впровадження ефективних й інноваційних методів боротьби з цими загрозами.

Важливо розуміти, що шкідливі програми постійно еволюціонують, використовуючи нові техніки та стратегії для обходу механізмів захисту комп'ютерних систем. Це вимагає постійного оновлення та вдосконалення методів виявлення та нейтралізації цих загроз.

Нові технології, такі як машинне навчання та штучний інтелект, відкривають нові можливості для ефективного виявлення та боротьби зі шкідливими програмами. Алгоритми машинного навчання можуть виявляти аномалії та нетипову поведінку програм, що можуть свідчити про їхню шкідливість, тоді як штучний інтелект може аналізувати великі обсяги даних для виявлення складних поведінкових патернів.

Однак успішна боротьба з шкідливими програмами також потребує спільних зусиль від кібербезпекових фахівців, розробників програмного забезпечення та, особливо, кінцевих користувачів. Важливою є постійна увага до цієї проблеми та розвиток нових стратегій та підходів для забезпечення цифрової безпеки та захисту користувача в мережі Інтернеті. Тільки завдяки глобальній кооперації та спільним зусиллям можливо забезпечити безпеку та приватність у цифровому світі для всіх користувачів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Вільям Столлінгз. "Cryptography and Network Security: Principles and Practice", 2022. - 784 с.
2. Машинне навчання. Електронний ресурс. Режим доступу: https://uk.wikipedia.org/wiki/ Машинне_навчання
3. Пам'ятка з кібербезпеки. Електронний ресурс. Режим доступу: https://www.it.ua/news/pamjatka-po-kiberbezopasnosti
4. 10 найбільших проблем використання AI у сфері кібербезпеки. Електронний ресурс. Режим доступу: https://aw.club/global/uk/blog/10-most-critical-ai-challenges-in-cybersecurity
5. Vectra AI - Штучний інтелект зупиняє хакерів. Електронний ресурс. Режим доступу: https://nwu.com.ua/bloh/statti/vectra-al-shtuchnyi-intelekt-zupyniaie-khakeriv

Семенюк Андрій Васильович - Інститут докторантури та аспірантури, Вінницький національний технічний університет, м. Вінниця, e-mail: andrew.semeniuk.university@gmail.com

Semeniuk Andrew V. - Institute of doctoral and postgraduate studies, Vinnytsia National Technical University, Vinnytsia, e-mail: andrew.semeniuk.university@gmail.com