УДК 004.056.5

А.В. Семенюк

МЕТОДИ ВИЯВЛЕННЯ ШКІДЛИВИХ ПРОГРАМ

Вінницький національний технічний університет

Анотація

Заради забезпечення кібербезпеки та захисту інформаційних систем від зловмисного втручання важливо виявляти та ідентифікувати шкідливі програми. Ця стаття розглядає методи виявлення шкідливих програм, а також їхню роль у попередженні кіберзагроз та забезпеченні безпеки інформації.

Ключові слова: шкідливі програми, виявлення загроз, кібербезпека, антивірусне програмне забезпечення, сигнатурний аналіз, поведінковий аналіз.

Abstract

In order to ensure cyber security and protect information systems from malicious interference, it is important to detect and identify malicious programs. This article examines malware detection techniques and their role in cyber threat prevention and information security.

Key words: malware, threat detection, cyber security, antivirus software, signature analysis, behavioral analysis.

Вступ

В сучасному світі, що досить стрімко розвивається в галузі інформаційних технологій, кібербезпека стала однією з найбільш актуальних і нагальних проблем. Інформаційні системи, комп'ютери та цифрові мережі стали невід'ємною частиною нашого повсякденного життя. Із зростанням цифрового світу з'явилася загроза безпеці даних, що у великих обсягах зберігаються, трансформуються та переміщуються.

Шкідливі програми, кібератаки, інформаційні витоки і інші аспекти кібербезпеки стали важливою проблемою для організацій, урядів і окремих користувачів. Зловмисники, які використовують різноманітні техніки для порушення безпеки, завдають значних збитків як корпоративному, так і урядовому сегментам.

Метою дослідження є розгляд методів виявлення шкідливих програм та їхньої ролі в забезпеченні кібербезпеки. Буде розглянуто основні підходи та техніки, які використовуються для ідентифікації шкідливих програм, їх переваги та обмеження.

Об’єктом дослідження є методи виявлення шкідливих програм та їхній вплив на кібербезпеку.

Предметом дослідження є вплив шкідливих програм на безпеку інформаційних систем, методи їх виявлення та запобігання.

Головною задачею є огляд і пояснення основних методів виявлення шкідливих програм, включаючи сигнатурний аналіз, поведінковий аналіз та машинне навчання. Також буде розглянуто переваги та обмеження кожного методу.

Методи виявлення шкідливих програм

Сигнатурний аналіз. Сигнатурний аналіз використовує попередньо визначені сигнатури шкідливих програм для ідентифікації відомих загроз. Ці сигнатури є унікальними хеш-сумами або паттернами байтів, які можуть ідентифікувати конкретну шкідливу програму. Коли антивірусне програмне забезпечення або інший захисний продукт знаходить файл у системі, воно порівнює хеш-суму цього файлу із вже відомим списком сигнатур. Якщо виявляється відповідність, то файл визнається як шкідливий і може бути відокремлений або видалений із системи.

Однак цей метод має декілька обмежень. Він може ефективно виявляти лише відомі загрози, але не може впізнавати нові чи перероблені варіанти шкідливих програм. Також, оновлення списку сигнатур вимагає постійного моніторингу та оновлень від розробників антивірусного програмного забезпечення.

Поведінковий аналіз. Поведінковий аналіз є одним із методів виявлення шкідливих програм і загроз в інформаційних системах. Цей підхід не базується на виявленні конкретних сигнатур чи паттернів файлів, як, наприклад, у сигнатурному аналізі, але замість цього аналізує активність програм та їхні зміни в системі. Основна ідея полягає в тому, що шкідливі програми часто проявляють певну небажану або підозрілу активність, яка може бути ідентифікована та виявлена на рівні їхньої поведінки.

Основні аспекти поведінкового аналізу включають:

- моніторинг активності програм – в рамках поведінкового аналізу відбувається моніторинг активності програм, які працюють в системі. Це включає в себе спостереження за тим, які файли вони відкривають, які системні ресурси вони використовують та як вони взаємодіють з іншими програмами;

- виявлення аномалій – поведінковий аналіз спрямований на виявлення аномалій у системі. Це може включати виявлення незвичайних або підозрілих дій, таких як спроби модифікації системних файлів, спроби виконати шкідливий код, або спроби звертатися до мережевих ресурсів без відома користувача системи;

- аналіз змін – поведінковий аналіз аналізує зміни, внесені програмою в систему. Це може включати в себе виявлення спроб створення нових файлів, модифікацію системних параметрів, чи інші дії, які можуть вказувати на шкідливу активність;

- реакція на підозрілу активність – якщо система виявляє підозрілу активність, вона може вживати заходів для ізоляції або блокування програми, яка виконує цю активність. Це може включати в себе відключення програми від мережі, блокування її доступу до файлів або навіть повне видалення програми;

Переваги поведінкового аналізу включають здатність виявляти нові атаки, які не мають відомих сигнатур, а також здатність до аналізу в реальному часі. Однак, цей метод також може викликати певну кількість помилкових спрацювань, вимагає більше обчислювальних ресурсів порівняно із сигнатурним аналізом. Загалом, поведінковий аналіз є важливим інструментом в сфері кібербезпеки, оскільки він допомагає виявляти загрози, які можуть бути невідомими або які змінюють свою поведінку з часом.

Машинне навчання. Машинне навчання в контексті кібербезпеки грає важливу роль у виявленні, захисті та реагуванні на різноманітні кіберзагрози. Використання методів машинного навчання дозволяє автоматизувати та покращити простір кібербезпеки, оскільки ці методи можуть аналізувати великі обсяги даних та виявляти аномалії з загрозами, які можуть бути недоступними для звичайного людського аналізу. Ось деякі основні способи використання машинного навчання в кібербезпеці:

- виявлення аномалій – машинне навчання може використовуватися для виявлення аномальної активності в мережах та системах, адже моделі навчаються на основі нормальної поведінки, а потім вони можуть виявляти аномалії, які можуть свідчити про потенційні загрози;

- виявлення шкідливого програмного забезпечення – машинне навчання може допомогти виявляти шкідливе програмне забезпечення, включаючи віруси, троянські програми, хробаків та інші загрози, навіть якщо вони є новими чи не мають відомих донині сигнатур;

- аналіз потоків даних – машинне навчання може аналізувати великі потоки даних в реальному часі та виявляти небажану або підозрілу активність, що є доволі важливим для захисту мережі та реагування на атаки в режимі реального часу;

- ідентифікація і аутентифікація користувачів – машинне навчання допомагає виявляти небажану активність та відслідковувати спроби несанкціонованого доступу до системи;

- аналіз поведінки користувачів – машинне навчання може визначати зміни в поведінці користувачів, що може вказувати на крадіжку акаунта або подібні загрози;

- реагування на інциденти – машинне навчання може допомогти автоматизувати процес реагування на кіберінциденти, включаючи ізоляцію певних систем та реагування на атаки в реальному часі;

- прогнозування загроз – машинне навчання може використовуватися для аналізу трендів та прогнозування майбутніх кіберзагроз;

- аналіз великих об'ємів даних – великі обсяги даних можуть бути аналізовані з використанням методів машинного навчання для виявлення важливих закономірностей та залежностей.

Важливо враховувати, що машинне навчання не є універсальним засобом для вирішення всіх проблем в кіберпросторі й вимагає належного налаштування і підтримки. Також, забезпечення безпеки даних та моделей машинного навчання є важливою складовою використання цих методів в кібербезпеці. Також цей спосіб захисту вимагає тренувальних даних і постійного оновлення моделей, що є затратними операціями.

Висновки

Методи виявлення шкідливих програм відіграють важливу роль у забезпеченні кібербезпеки. Комбінування різних підходів, таких як сигнатурний аналіз, поведінковий аналіз і машинне навчання може забезпечити більш ефективний захист інформаційних систем від шкідливих програм. Однак важливо пам'ятати, що загрози в постійному розвитку, тому постійне оновлення інструментів захисту та удосконалення методів виявлення є необхідними для збереження кібербезпеки. Безпека інформації стає все більш важливою, тому виявлення шкідливих програм є однією з ключових складових її забезпечення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Росс Андерсон. Security Engineering: A Guide to Building Dependable Distributed Systems, 2020. – 1232 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

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