DOI: 10.59647/978-617-520-936-3/1

Аналіз сучасного шкідливого програмного забезпечення та методи боротьби з ним

Дмитро Піддубний, студент [1] (ORCID: 0009-0008-0405-1928)**, Євгенія Шабала,** к.т.н., доц.[1] (ORCID: 0000-0002-0428-9273)

[1] *Київський національний університет будівництва і архітектури, 03037, м. Київ, проспект Повітряних Сил, 31, Україна*

АНОТАЦІЯ

У роботі розглянуто сучасні види шкідливого програмного забезпечення. Проведено аналіз методів їх поширення та впливу на інформаційні системи. Окремо досліджено сучасні підходи до боротьби зі шкідливим програмним забезпеченням, зокрема статичний та динамічний аналіз, поведінкові методи, а також використання машинного навчання для виявлення загроз.

Ключові слова: шкідливе програмне забезпечення, вірус, хробак, троян, антивірус, дані, аналіз, файл, загроза.

1. ВСТУП

Шкідливе програмне забезпечення є однією з найсерйозніших загроз в галузі кібербезпеки. Його основна мета – порушення роботи комп'ютерних систем, крадіжка даних або отримання неправомірного доступу до інформаційних ресурсів. Розвиток шкідливого програмного забезпечення відбувається разом із розвитком технологій, і сучасні кіберзагрози стають все складнішими та небезпечнішими.

2. МЕТА РОБОТИ

Робота присвячена питанню шкідливого програмного забезпечення та методів боротьби з ним. В роботі представлені основні визначення, вити шкідливого програмного забезпечення та наведено методи боротьби з ним.

3. ОСНОВНІ ВИЗНАЧЕННЯ

Шкідливе програмне забезпечення – це програмне забезпечення, створене для реалізації загроз даним, що зберігаються в інформаційній системі, або для прихованого нецільового використання ресурсів системи, або інших дій, що перешкоджають правильному функціонуванню інформаційної системи. Зазвичай воно здатне поширюватись і заражати додаткові інформаційні системи.

Комп'ютерні віруси – це програми, здатні записувати свій код у код інших програм, створювати свої дублікати та виконувати несанкціоновані дії на комп'ютері.

Хробаки комп'ютерних мереж – пересилають свої копії комп'ютерними мережами з метою проникнення на віддалені комп'ютери.

Троянські програми – це програми, що проникають на комп'ютери користувачів разом з програмами, які користувач «отримує» комп'ютерними мережами.

Антивірусні програми – спеціалізоване програмне забезпечення для захисту даних і комп'ютерних систем від шкідливих програм.

4. ВИДИ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Для шкідливого програмного забезпечення характерні такі дії:

1. Швидке розповсюдження шляхом приєднання копій своїх даних до інших програм, копіювання на інші носії даних, пересилання копій по комп'ютерній мережі.
2. Автоматичне виконання дій, які вносять негативні зміни в роботу комп'ютера:

- Знищення даних шляхом видалення файлів певних типів або форматування дисків;
- Внесення змін у файли, зміна структури розміщення файлів на диску;
- Зміна або повне видалення даних із постійної пам'яті;
- Зниження швидкодії комп'ютера, наприклад за рахунок заповнення оперативної пам'яті своїми копіями;
- Примусове перезавантаження операційної системи;
- Блокування запуску певних програм;
- Збирання і розповсюдження копій даних комп'ютерними мережам, наприклад пересилання кодів доступу до секретних даних;
- Використання ресурсів вже заражених комп'ютерів для проведення атак на інші комп'ютери в мережі;
- Виведення звукових або текстових повідомлень, спотворення зображення на екрані, тощо.

За рівнем небезпеки дії шкідливого програмного забезпечення поділяються на:

- Безпечні – проявляються звуковими або відео ефектами, не змінюють файлову систему, не шкодять файлам і не виконують шпигунських дій;
- Небезпечні – призводять до некоректної роботи комп'ютерної системи: зменшують розмір оперативної пам'яті, перезавантажують систему, тощо;
- Дуже небезпечні – знищують дані з постійної та зовнішньої пам'яті, виконують шпигунські дії, тощо.

Класифікація шкідливого програмного забезпечення за принципом розповсюдження та функціонування.

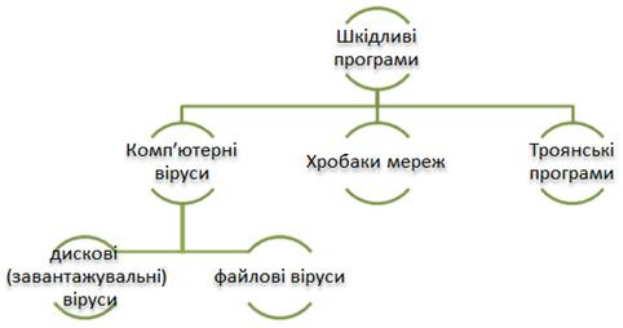

Рисунок 1 Класифікація шкідливих програм

Віруси – це програма, яка може самовідтворюватися, впроваджуючись в файли та програми. Вірус може поширюватись через зовнішні носії, електронну пошту, завантаження будь чого з інтернету, тощо.
За середовищем існування віруси розподіляються на:

- Дискові (завантажувальні) віруси – це віруси, які інфікують завантажувальні сектори жорстких дисків або інших носіїв даних, таких як флеш-накопичувачі та оптичні диски. Вони запускаються під час завантаження операційної системи, що дозволяє їм непомітно для антивірусних програм активуватись.
- Файлові віруси – віруси, які знаходяться у файлах операційної системи комп'ютера. Дані віруси являють собою блоки програмного коду, які додають себе до коду інших програм і таким чином змінюють функціонал програми.
- Макровіруси – це віруси, які написані мовою програмування макросів, яка вбудована в офісний пакет Microsoft Office. Макровіруси здатні інфікувати документи та автоматизовані процеси в програмах, виконуючи шкідливі дії, коли користувач відкриває заражений вірусом файл.

Хробаки – це шкідливі програми, які можуть самостійно поширюватися по мережам, використовуючи вразливості в програмному забезпеченні. Вони можуть завантажувати інші шкідливі програми, або здійснювати DDoS – атаки. Більшість хробаків поширюються шляхом прикріплення до файлів електронної пошти, електронних документів, тощо.

Трояни – це шкідливі програми, які маскуються під корисне або легальне програмне забезпечення, але виконують шкідливі дії, такі як крадіжка даних або встановлення інших шкідливих програм.

Руткіти – програми, що приховують присутність шкідливого програмного забезпечення в системі, змінюючи системні файли та процеси. Можуть забезпечувати зловмисникам несанкціонований доступ до мережі.

Шпигунське програмне забезпечення – це програми, які збирають інформацію про користувача бей його відома, такою інформацією є історія браузера, особисті дані, банківські дані, тощо і передають її зловмисникам.

Backdoor – це програми або методи, які дозволяють зловмисникам отримати несанкціонований доступ до системи, оминаючи стандартні механізми автентифікації.

Програми-вимагачі – це програми, які шифрують файли користувача або блокують доступ до системи, вимагаючи викуп за відновлення доступу.

5. МЕТОДИ ВИЯВЛЕННЯ ТА БОРОТЬБИ З ШКІДЛИВИМ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ

Антивірусні програми – це спеціальне програмне забезпечення створене для захисту даних і комп'ютерних систем від шкідливих програм. Антивірусні програми до складу операційної системи не входять, їх треба встановлювати окремо, в більшості випадків дійсно працююча антивірусна програма буде платною.

Зазвичай антивірусні програмні пакети мають в своєму складі:

- Програму-сканер, яка переглядає всі файли, сектори пам'яті з метою пошуку унікального програмного коду, тобто вірусу;
- Антивірусний монітор, який автоматично завантажується в оперативну пам'ять після запуску комп'ютера та виконує перевірку на віруси всіх файлів, з якими ведеться робота;
- Ревізор змін, який запам'ятовує певні дані кожного файлу. Ці дані зберігаються окремо та при кожному завантаженні файлу і його зміні ревізор порівнює дані та повідомляє про зміни;
- Засоби оновлення антивірусних баз через Інтернет, які дозволяють своєчасно виявляти та знищувати нові комп'ютерні віруси.

Статичний аналіз. Полягає в аналізі коду програмного забезпечення без його виконання. Антивірусні програми сканують файли на наявність підозрілих сигнатур та унікального програмного коду. Може бути неефективним проти програмного забезпечення, яке змінює свій код для уникнення виявлення.

Динамічний аналіз. Вивчає поведінку шкідливого програмного забезпечення під час виконання в контрольованому середовищі, це дозволяє виявляти навіть замасковане шкідливе програмне забезпечення.

Методи на основі поведінкового аналізу. Зосереджені на відстеженні аномальної поведінки програм в системі. Виявляють дії, які характерні для шкідливого програмного забезпечення, наприклад спроби змінити системні файли або передача даних до невідомих адресатів.

Машинне навчання. Використання алгоритмів машинного навчання для аналізу великих масивів даних і виявлення нових загроз. Штучний інтелект навчається на основі існуючих зразків шкідливого програмного забезпечення і здатен знаходити аномалії, які можуть вказувати на нові типи загроз.

6. ВИСНОВОК

Сучасне шкідливе програмне забезпечення стає дедалі складнішим, використовуючи новітні методи для обходу захисту та маскування. Однак разом із розвитком кіберзагроз розвиваються й методи їх виявлення та боротьби. Використання багаторівневого захисту, що включає статичний і динамічний аналіз, машинне навчання та поведінковий аналіз, є ключовим підходом до забезпечення кібербезпеки.

Список літератури

[1] Діагностика шкідливого програмного забезпечення: методичні вказівки для підготовки до підсумкового контролю. [Електронний ресурс] / укладач Л. Я. Глинчук; ВНУ ім. Лесі Українки. Електронні текстові данні. Луцьк : ВНУ ім. Лесі Українки, 2023. 74 с.

[2] Програмне забезпечення та інформаційна безпека. URL: https://www.miyklas.com.ua/p/informatica/9-klas/programne-zabezpechennia-ta-informatciina-bezpeka-327110

[3] Черкун О.М.. Сучасні технології комп'ютерної безпеки. Монографія. МЕГУ, Рівне, 2012. – 90с.

[1] *Робота виконана під керівництвом к.т.н. доц. Євгенії Шабали.*