Секція 1

ПОЛІМОРФНІ ВІРУСИ ТА МЕТОДИ ЇХ ВИЯВЛЕННЯ

Родіонов Д. В.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Пєвнєв В. Я.

Актуальність. Тема вірусів стає все більш актуальною з кожним роком, тому що кількість користувачів комп'ютерами та мережею Інтернет збільшується. Дуже часто у інтернеті разом із корисним матеріалом можна підхопити багато різноманітних вірусів. Відповідно до популяризації комп'ютерів, спеціалісти з кібербезпеки турбуються про безпечність користування Інтернетом та відповідні протидії вірусам. На даний момент є багато антивірусних програм, які знаходять та видаляють віруси [1]. Але з кожним роком створюється безліч нових вірусів, і модіфікуються старі, саме тому антивірусні програми просто не встигають за ними. Одним із типів захищеності вірусів є поліморфізм вірусів.

Метою даної роботи є дослідження поліморфних вірусів та методів їх виявлення.

Основні положення. Поліморфні віруси запрограмовані таким чином, що вони можуть змінювати тіло вірусу після чергового зараження [2]. Найчастіше зміна коду досягається шляхом додавання операторів, які не змінюють принцип роботи вірусу. Підхід до виявлення саме поліморфних вірусів суттєво відрізняється від виявлення інших типів вірусів. Для того щоб знайти та ліквідувати поліморфний вірус, потрібно знати як він працює.

Кожен вірус має характерні ознаки. Такими ознаками можуть бути дії, що виконуються самим вірусом, характерними ознаками є ціль вірусу та методи її досягнення. На основі такої інформації і складаються сигнатури вірусів, використовуючи які антивірус шукає шкідливі програми. Також антивірус може ізолювати вірус (запуск в режимі sandbox) і вже там спостерігати за його поведінкою [3].

Існує багато технологій виявлення вірусів. Їх можна поділити на 2 групи [4].: технології сигнатурного аналізу та технології імовірнісного аналізу: сигнатурний аналіз - метод виявлення вірусів , що полягає в перевірці наявності в файлах сигнатур вірусів; евристичний аналіз -

технологія, заснована на імовірнісних алгоритмах, результатом роботи яких є виявлення підозрілих об'єктів.

У процесі евристичного аналізу перевіряється структура файлу, його відповідність вірусним шаблонах. Найбільш популярною евристичної технологією є перевірка вмісту файлу на предмет наявності модифікацій уже відомих сигнатур вірусів та їх комбінацій. Це допомагає визначати гібриди і нові версії раніше відомих вірусів без додаткового оновлення антивірусної бази. Евристичний аналіз - один із методів виявлення поліморфних вірусів.

Аналіз контрольних сум - це спосіб відстеження змін в об'єктах комп'ютерної системи. На підставі аналізу характеру змін - одночасність, масовість, ідентичні зміни довжин файлів - можна робити висновок про зараження системи.

Висновки. Поліморфні віруси майже неможливо виявити сигнатурними антивірусами. Для виявлення даного виду зловмисних програм потрібно відстежувати поведінку вірусу та фіксувати усі види підозрілої активності. Найкраще для цього підходить евристичний аналіз та аналіз контрольних сум. Як один із варіантів захисту від потрапляння поліморфних вірусів є резидентні монітори.

Список літератури

1. Новаков Е.О., Цуранов М.В. Использование обучаемых HIPS-антивирусов для противодействия киберпреступности. Системи управління, навігації та зв'язку, 2017, випуск 1(41).
2. Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційній сфері: навчальний посібник / М.В. Цуранов, В.М. Струков, В.Я. Пєвнєв. – Харків: ХНУВС, 2015. – 256 с.
3. Polymorphic virus. *Cyber Hoot*. URL – https://cyberhoot.com/cybrary/polymorphic-virus/ (дата звернення: 20.11.2021);
4. Полиморфизм компьютерных вирусов. *Рус наука*. URL: http://www.rusnauka.com/14_NPRT_2010/Informatica/66880.doc.htm (дата звернення: 20.11.2021).

Відомості про авторів

Родіонов Дмитро Валерійович, студент кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 098-026-47-48, d.rodionov@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, доцент кафедри комп’ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu