АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Тютюнник М.В., студент, mykola.tiutiunnyk1.kita@donntu.edu.ua
Мороз Є.З., студент, yevhen.moroz.kita@donntu.edu.ua
Рудською М.О., студент, mykyta.rudskoi.kita@donntu.edu.ua
Маслова Н.О., к.т.н., доцент, nataliia.maslova@donntu.edu.ua
Донецький національний технічний університет, Луцьк, Україна

Сьогоднішня технологічна епоха супроводжується не тільки нововведеннями та зручністю, але й загрозами від шкідливих програм. Щодня мільйони користувачів стикаються з ризиком інфікування своїх пристроїв та систем шкідливим програмним забезпеченням. Саме тому аналіз шкідливих програм стає надзвичайно важливим для сучасного цифрового світу.

Що таке аналіз шкідливих програм? Шкідливе програмне забезпечення, часто відоме як malware, складається з різноманітних програм, спрямованих на завдання шкоди комп'ютерним системам, даним користувачів та навіть цілій мережі. Аналіз шкідливих програм полягає в дослідженні, виявленні та розумінні цих вірусів, хробаків, троянців та інших зловмисних програм.

Чому аналіз шкідливих програм настільки важливий? Перш за все, аналіз дозволяє розуміти та передбачати можливі загрози для інформаційної безпеки. Він допомагає розробникам антивірусних програм та програмістам уникнути вразливостей, а також забезпечує організаціям та користувачам кращий захист від потенційно небезпечних програм [1].

Типи аналізу шкідливих програм. Існують різні методики аналізу шкідливих програм, як то:

- статичний аналіз (оцінка програмного коду без його виконання - цей метод дозволяє виявляти потенційно шкідливі функції або вразливості);
- динамічний аналіз (вивчення поведінки програми під час її виконання - це дозволяє виявити зміни в системі, спричинені шкідливими програмами);
- поведінковий аналіз (аналізується тільки функціонування програми, не звертаючи увагу на її внутрішній код - це допомагає виявити зміни в системі, що можуть бути спричинені шкідливими програмами).

Інструменти для аналізу шкідливих програм. Щоб здійснювати аналіз шкідливих програм, використовуються різноманітні інструменти [2].

Антивіруси та антишпигуни. Вони призначені для виявлення та блокування шкідливих програм перед їх виконанням.

Дебагери та дизасемблери. Засоби використовуються для дослідження роботи програми в процесі виконання та аналізу машинного коду.

Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS). Це програмне забезпечення моніторить мережевий трафік та виявляють потенційно шкідливі дії.

Таким чином, для аналізу роботи та характеристик шкідливого програмного забезпечення, оцінювання його впливу на комп'ютерну систему застосовують різні методи та інструментальні засоби. Аналіз шкідливих програм - це вивчення поведінки шкідливого шкідливих програм, способів зараження комп'ютерної системи, а також пошук методи виявлення шкідливого програмного забезпечення та усунення як самих вірусів, так й наслідків їх діяльності. Одним з методів аналізу підозрілого програмного забезпечення є його дослідження у спеціально створеному захищеному віртуальному середовищі [3].

Архітектура віртуального середовища. Для створення віртуального середовища, у якому буде проводитись дослідження шкідливих програм була розгорнута хост-машина під керуванням Ubuntu Linux з екземплярами віртуальної машини Ubuntu Linux VM і віртуальної машини Windows VM. Віртуальна машина Windows - місце, де шкідлива програма буде виконуватися під час аналізу, а віртуальна машина Linux використовується для моніторингу мережевого трафіку. Віртуальні машини повинні бути частиною однієї мережі, використовувати режим конфігурації мережі host-only. Віртуальні машини слід налаштувати так, щоб шкідливі програми не змогли вийти в інтернет, а мережевий трафік не повинен виходити за межі ізольованого тестового середовища.

Опис процесу встановлення й налагодження тестового віртуального середовища склався приблизно з восьми послідовних кроків.

Першим кроком є набуття адміністратором прав для вводу команд та завантаження apt, оновлення всіх необхідних програм.

Надалі слід встановити програмне середовище pip - це система управління пакетами, яка використовується для установки і управління пакетів, написаних на Python для завантаження python.

Наступний крок налаштувань - встановлення python3, upx, pefile, yara та yara-python. Ці кроки необхідні для встановлення програмного забезпечення ssdeep.

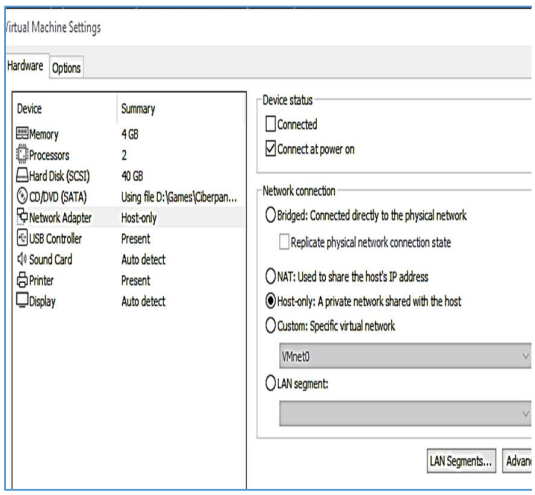

Рисунок 1. Включення режиму host-only

Щоб налаштувати wireshark та оновити програму до tshark, було встановлено бібліотеки.

Слід врахувати, що службу захисту на віртуальній машині Windows необхідно буде відключити, так як вона може перешкоджати запуску та дослідженню зразку шкідливого ПО.

Надалі, для того щоб заблокувати доступ до передачі даних на основний комп'ютер, слід виконати

зміну файлів реєстру й для налаштування Інтернет зв'язку встановити програму inetsim. Її наявність дозволить включити режим host-only, як показано на рисунку 1.

Рисунок 2. Активований вірус

Тепер завантажимо вірус з середовища theZOO. TheZoo — це проект, створений для того, щоб зробити можливість аналізу зловмисного програмного забезпечення відкритою та доступною для дослідників [4]. Активація вірусів відбувається у терміналі, після чого з'являється деякий малюнок. Паспорт та зовнішній прояв роботи вірусу наведено на рисунку 2. Цей вірус є не дуже небезпечним, тому система не ламається повністю, але починає працювати повільно, її робота гальмується.

Висновок. Аналіз шкідливих програм є критично важливим для забезпечення безпеки в цифровому світі. З розвитком технологій він стає все складнішим, але вдосконалені методи аналізу та ефективні інструменти дозволяють дослідникам активніше реагувати на виклики та захищати системи від потенційних загроз.

Література

1. Терейковський І.А. Методи розпізнавання кібератак: розпізнавання комп'ютерних вірусів / І.А. Терейковський, О.Г. Корченко, В.В. Погорелов. — Київ: КПІ ім. Ігоря Сікорського, 2022. — 127с.

2. Практикум із загальної вірусології / за ред. О.Л. Бійка. . — К.: Видавничий центр „Київський університет", 2000. . — 269 с.

3. Monnappa K A, Learning Malware Analysis: Packt Publishing Ltd., 2018. . — 501p

4. Yuval Nativ. TheZoo - A Live Malware Repository. 2015. url: https://thezoo.morirt.com/

Анотація

У статті описано один з сучасних методів дослідження шкідливих програм, їх проявів та поведінки. Це метод розгортання тестового віртуального середовища. Віртуальне середовище забезпечує ізольованість операційної системи основного комп'ютера від шкідливого впливу, дослідник має можливість повноцінно виконувати всі необхідні роботи з аналізу шкідливих програм, отримувати навички з їх знешкодження.

Ключові слова: програма, вірус, віртуальна машина, Linux, Python, theZoo.

Abstract

The article describes one of the modern methods of researching malicious programs, their manifestations and behavior. This is a deploy test virtual environment method . The virtual environment ensures the isolation of the operating system of the main computer from harmful effects, the researcher has the opportunity to fully perform all the necessary work on the analysis of malicious programs, to acquire skills in their elimination.

Keywords: program, virus, virtual machine, Linux, Python, theZoo.