Секція 1

АНТИВІРУСНИЙ ЗАСІБ ДЛЯ ВИЯВЛЕННЯ СТЕЛС-ВІРУСІВ

Шипунов М.Ю.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник: ст. викладач Цуранов М. В.

Актуальність. На сьогоднішній день, завдяки розповсюдженості мережі Інтернет, все частіше відбуваються масові вірусні зараження інфокомунікаційних систем, що наносить величезні збитки. Лише кількість атак з використанням вірусів типу Ransomware збільшилось на 46% [1]. Кількість знайдених вірусів-майнерів збільшилась на 8500% [1]. На 80% збільшилася кількість знайдених вірусів під MacOS [1]. Згідно звіту компанії Symantec, кількість офіційно зареєстрованих вразливостей збільшилася на 13% [1]. На 92% збільшилась кількість заблокованих завантажувальних вірусів [1]. У 2017 році найбільш серйозна атака проводилася з використанням вірусу WannaCry (> $1 млрд збитків) [2].

Мета роботи: полягає у аналізі механізмів роботи стелс вірусів та існуючих засобів для боротьби з ними.

Основні положення. За особливостями алгоритму роботи, віруси поділяються на наступні категорії: резидентні, поліморфні та стелс [3]. Найбільш небезпечні віруси мають стелс елементи, тому що найбільші збитки були нанесені саме шкідливим програмним забезпеченням, яке використовувало цю технологію.

Проблема виявлення стелс-вірусів полягає в тому, що вони активно ховають свою присутність у системі шляхом перехоплення системних повідомлень або підміни деяких компонентів операційної системи [3]. Через це, коли виконується системний виклик або відкриття файлу, вірус перехоплює контроль та окрім реальних функцій системи, виконує свої [3]. Для того, щоб знайти та деактивувати вірус, потрібен антивірус, який буде ефективний проти стелс вірусів. За технологіями захисту класифікують наступні антивірусні засоби: сигнатурні, проактивні та комбіновані [3].

Сигнатурні антивіруси під час пошуку використовують для виявлення вірусів бази даних, та здебільшого не є ефективними під час пошуку вірусів зі стелс елементами [3]. Це зумовлено тим, що процес оновлення та додавання нових сигнатур у бази потребує часу.

У свою чергу проактивні антивіруси намагаються запобігти зараженню комп'ютера, замість того, щоб шукати вірус у вже зараженій системі. Ефективність такого антивірусу залежить від проактивної компоненти яка

в ньому використовується. Найпоширенішими алгоритмами проактивного захисту є: евристичний аналіз, емуляція коду, виконання коду у пісочниці та віртуалізація робочого оточення для аналізу поведінки [4]. Найбільш дійовою вважається виконання програм у пісочниці, так як програма виконується в ізольованому місці та не може завдати шкоди системі. Основним недоліком проактивних антивірусів є помилкові спрацювання. Через це користувач може заблокувати роботу антивірусного програмного забезпечення після декількох повідомлень про зараження.

Комбіновані антивіруси поєднують різні підходи. До них відносяться як сигнатурний пошук так і проактивні технології, які було розглянуто вище. Наразі більшість антивірусного програмного забезпечення використовують комплексний підхід для захисту комп'ютера. Прикладом таких антивірусів є: Zillya! Total Security, Kaspersky Internet Security та Avast! Antivirus.

Висновки. Аналіз особливостей роботи стелс вірусів та антивірусного програмного забезпечення показав, що існуючі методи захисту не можуть гарантовано виявляти стелс віруси. Найбільш ефективними себе показали антивіруси з проактивними компонентами, але і вони не можуть безпомилково знешкодити віруси даного типу. Саме тому є необхідність в створенні спеціального антивірусного засобу, який комбінував використання декількох проактивних компонент для збільшення ймовірності виявлення та знешкодження в системі стелс вірусів.

Список літератури

1. Symantec Internet Security Thread Report. Volume 38. *Symantec*. URL – https://docs.broadcom.com/doc/istr-23-2018-en (дата звернення: 20.10.2021);
2. Убытки от WannaCry оценили в миллиард долларов. *Економічна правда.* URL: https://www.epravda.com.ua/rus/news/2017/05/25/625286/ (дата звернення: 2.11.2021);
3. 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.;
4. Новаков Е.О., Цуранов М.В. Использование обучаемых hips-антивирусов и для противодействия киберпреступности. Системи управління, навігації та зв'язку, 2017, випуск 1(41).

Відомості про авторів

Шипунов Микита Юрійович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 098-034-43-88, m.shypunov@student.csn.khai.edu
Цуранов Михайло Віталійович, старший викладач кафедри комп'ютерних систем, мереж і кібербезпеки, m.tsuranov@csn.khai.edu