УДК 004.52

ДОСЛІДЖЕННЯ МЕТОДІВ ПОШУКУ ПОЛІМОРФНОГО ПРОГРАМНОГО КОДУ

К. т. н. О. С. Савенко, А. О. Нічепорук

Хмельницький національний університет
Україна, м. Хмельницький
nicheporuk90@gmail.com

В роботі досліджено методи діагностування комп'ютерних систем на наявність поліморфних вірусів. Розглянуто принципи функціонування поліморфних вірусів, а також методи їх виявлення. На основі аналізу сучасного стану антивірусних засобів виділено їх недоліки та переваги.

Ключові слова: *поліморфні віруси, обфускація, сигнатура.*

Розвиток інформаційних технологій дозволяє здійснювати інтеграцію розподілених обчислювальних та інформаційних ресурсів і надавати доступ до них великій кількості користувачів. Все це зумовило широке застосування інформаційних технологій в багатьох системах обробки інформації різного рівня та призначення. Однак мережна інтеграція призводить до збільшення ризиків користувачів, пов'язаних з можливістю розповсюдження по мережі шкідливого програмного забезпечення та одного з його різновидів – комп'ютерних вірусів, зокрема поліморфних вірусів.

Поліморфні віруси на сьогоднішній день залишаються одними з найбільш небезпечних. Поліморфні віруси модифікують свій код в уражених програмах таким чином, що два примірники одного і того ж вірусу можуть не співпадати жодним бітом [1, 3, 5, 6]. Такі віруси не тільки шифрують свій код, використовуючи різні шляхи шифрування, але й містять код генерації шифрувальника і розшифровувача, що відрізняє їх від звичайних шифрувальних вірусів, які можуть шифрувати ділянки свого коду, але мають при цьому постійний код шифрувальника і розшифровувача. Тому на сьогоднішній день поліморфні віруси представляють велику небезпеку для інформаційних систем. Відомі методи діагностування комп'ютерних систем на наявність поліморфного коду не дозволяють в повній мірі виявляти нові поліморфні віруси, або результат отримується за неприйнятно довгий проміжок часу, а також мають досить великий відсоток хибних спрацювань. Розробка методу для виявлення нових поліморфних вірусів, що дозволило б підвищити достовірність діагностування комп'ютерних систем на наявність таких вірусів, є актуальною.

Принципи функціонування поліморфних вірусів

Поліморфні віруси — це віруси в яких розшифровувач самомодифікується. Мета такого шифрування полягає у неможливості аналізу коду за допомогою дизасемблювання. Цей код зашифрований і представляє собою випадковий набір команд. Розшифровка відбувається самим вірусом вже безпосередньо під час виконання. При цьому можливі варіанти: він може розшифрувати себе всього відразу, а може виконати таку розшифровку у процесі свого виконання. Все це робиться з метою утруднення аналізу коду вірусу. Дані перетворення досягаються за допомогою процесу обфускації [1].

Обфускація – техніка, спрямована на заплутування коду програми, тобто вона приводить вихідний текст або виконуваний код до працюючого вигляду, але ускладнює аналіз такого коду. Так, створення заплутаного асемблерного тексту може бути досягнуто шляхом використання спеціалізованих компіляторів. Такі компілятори, зазвичай, заново створюють код, використовуючи для цього незадокументовані можливості середовища виконання програми [5].

Всі поліморфні віруси обов'язково містять розшифровувачі коду, які за певним принципом перетворюють переданий їм код, викликаючи при цьому стандартні функції і процедури операційної системи. Самі методи шифрування можуть бути різними, проте кожна операція, зазвичай, має свою дзеркальну пару. В асемблері це реалізується за допомогою пар команд – ADD/SUB, XOR/XOR, ROL/ROR і т. д. Подібні операції виконуються для розшифровки комірок пам'яті.

Важливою особливістю поліморфного вірусу є те, що вірус містить сміття, тобто операнди, функції та процедури, які слугують лише для заплутування коду.

Життєвий цикл поліморфного вірусу зображено на рис. 1. При старті зараженої програми вірусний поліморфний дескриптор розшифровує основне тіло вірусу та передає йому керування.

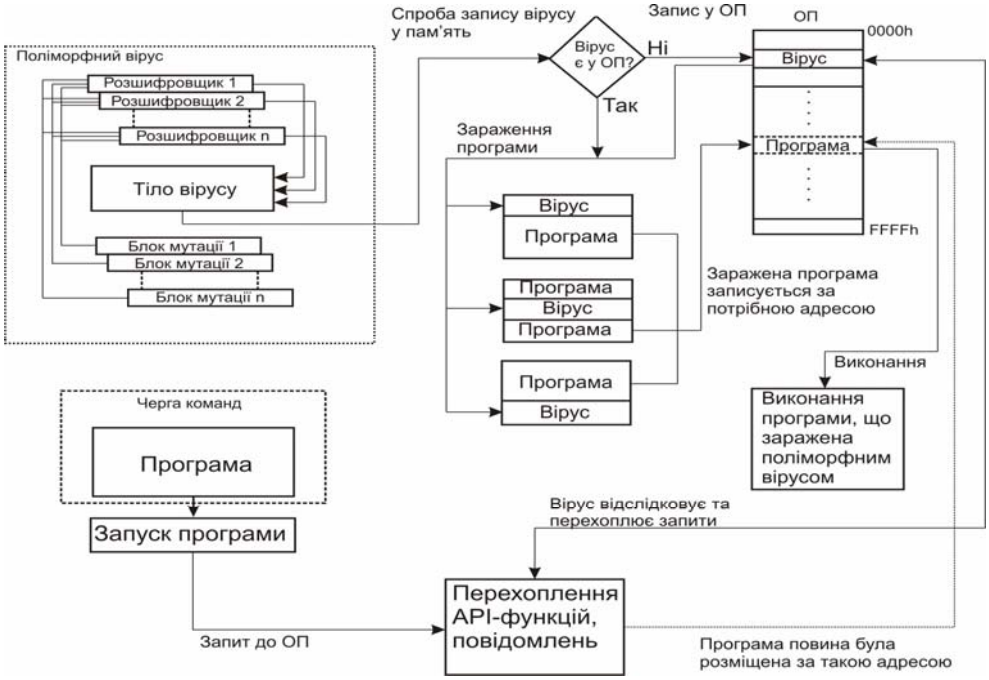

Рис. 1. Життєвий цикл поліморфного вірусу

Далі основний вірусний код виділяє ділянку пам’яті у верхніх адресах, копіює в нього власний код і передає йому керування. Потім він відновлює код зараженого файлу в програмному сегменті (для EXE-файлів також проводить налаштування адрес елементів, що переміщаються) і приступає до безпосереднього впровадження у пам’ять своєї резидентної копії. Після свого розміщення у пам’яті вірус виконує ряд підготовлених операцій для виділення пам’яті під своє тіло і проводить перемикання процесора в захищений режим роботи з найвищим рівнем пріоритету – режим супервізора. В процесі своєї роботи вірус може перехоплювати ряд системних ресурсів, зокрема API-функції, переривання, функції, що експортовані ядром ОС. Перехоплення API-функцій виконується через таблицю імпорту функцій. Дана таблиця заповнюється при завантаженні DLL в процес, і в ній прописуються адреси всіх імпортованих функцій, які процесу можуть знадобитися. Відповідно, вірус знаходить таблицю імпорту, в ній — функцію, яку він хоче перехопити, зберігає там адресу (покажчик на тіло функції), після чого розміщує туди покажчик на свою функцію. Далі він забороняє вивантаження DLL на час перехоплення (наприклад, DllCanUnloadNow повинна повертати false), щоб у процесі роботи DLL не була вивантажена, а адреса перехоплення не стала хибною.

Методи виявлення поліморфних вірусів

При пошуку поліморфних вірусів антивірусні програми використовують наступні методи: сигнатурний пошук, емуляція роботи процесора, евристичний аналіз [2].

Розглянуто сигнатурний пошук. Сигнатура вірусної програми — це фрагмент коду, що зустрічається у всіх копіях вірусу і тільки в них. Сигнатура однозначно визначає наявність або відсутність вірусу [6]. Виявлення, засноване на сигнатурах — методом роботи антивірусів і систем виявлення вторгнень, при якому програма, переглядаючи файл або пакет, звертається до словника з відомими вірусами, складеним авторами програми. У разі відповідності будь-якої ділянки коду програми, що переглядається, відомому коду (сигнатурі) вірусу в словнику, програма антивірус може зайнятися виконанням однієї з таких дій: видалити інфікований файл, відправити файл у «карантин», спробувати відновити файл, видаливши сам вірус з тіла файлу.

Розглянемо метод емуляції роботи процесора. Якщо код розшифровувача ”розбавлений” випадковою кількістю команд, які не впливають на процес розшифровки, то знайти постійну сигнатуру для такого розшифровувача неможливо [6].

До складу емулятора процесора входять програмні моделі основних пристроїв процесора і комп’ютера: черга команд, регістри загального призначення, сегментні регістри, основна пам’ять, файлова підсистема. Емулятор аналізує кожний наступний байт програми, виділяє керуючі поля, визначає формат команди, наявність і кількість операндів, обчислює адреси цих операндів. На основі цих даних емулюється виконання команд на програмних моделях частин комп’ютера, які змінює команда.

В основу методу евристичного аналізу покладено виявлення вірусу на основі заздалегідь відомих характеристик (евристик). Наприклад, для виявлення завантажувального вірусу, що прописаний в MBR (Master Boot Record), антивірус може зчитувати завантажувальний запис двома шляхами: функцією WinAPI ReadFile, або з використанням драйвера прямого доступу до диска (Direct Disk Access — DDA driver). А потім порівняти обидва буфера. Якщо буфери різні, то існує велика імовірність того, що в MBR є завантажувальний вірус [3,6].

Таблиця 1

Переваги та недоліки методів виявлення поліморфних вірусів

Метод виявлення поліморфних вірусів	Переваги	Недоліки
Сигнатурний пошук	Дозволяє визначити конкретну атаку з високою точністю і малою часткою хибних викликів	Нездатен виявити нові атаки; нездатен виявити видозмінену версію того ж вірусу; вимагає регулярного оновлення
Емуляція роботи процесора	Досить ефективне протистояння поліморфним вірусам за рахунок дій, а не програмного коду	Високе споживання системних ресурсів системи
Евристичний аналіз	Дозволяє виявити поліморфні віруси п’ятого і шостого рівнів	Наявність досить великого відсотку помилкових спрацювань [3]; наявність простих методів обходу евристики

На основі цих методів розроблено антивірусні програмні засоби різних виробників. Результати тестування програмних засобів на виявлення нових вірусів з використання методу евристики зображено на рис. 2 [3]. На рис. 3 зображено вплив евристичної складової та сигнатурного пошуку на виявлення поліморфних вірусів [4].

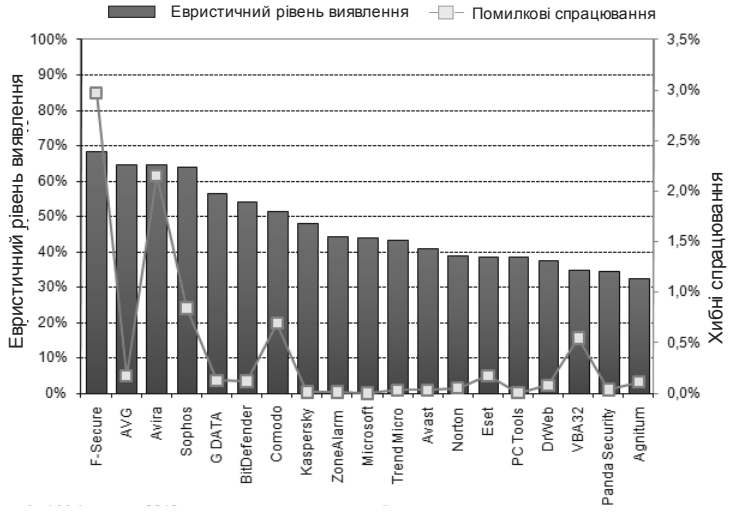

Рис. 2. Результати тесту евристичної складової антивірусу на виявлення нових вірусів [3]

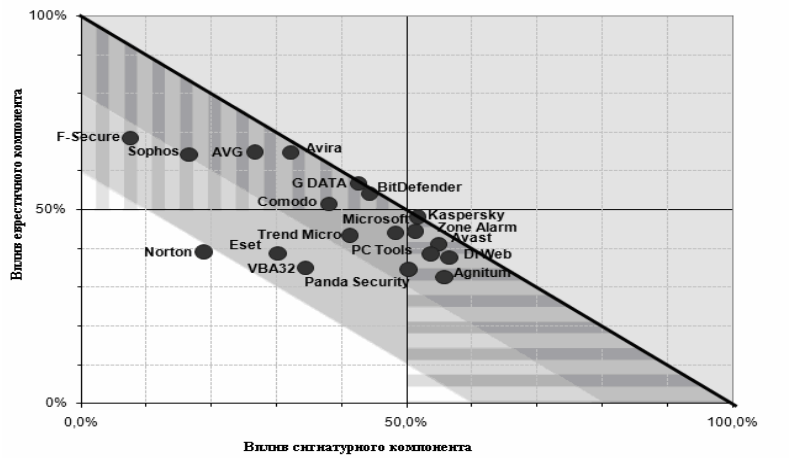

Рис. 3. Тест антивірусних засобів на виявлення поліморфних вірусів з використанням евристики та сигнатурного пошуку [4]

Результати тестування вказують, що використання евристики та сигнатурного пошуку не дає високої достовірності діагностування комп'ютерних систем на наявність нових вірусів.

Метод багатопрохідної емуляції полягає у багаторазовому виконанні поліморфного вірусу у віртуальному середовищі. Під час такого виконання поліморфний вірус повністю виконує свої дії (захоплення керування програмою, розгортання та ін.). Після того як поліморфний вірус виконає свої дії двічі, можна порівняти отримані сигнатури. Оскільки поліморфний вірус після свого виконання не утворює однакових сигнатур, то отримання двох різних сигнатур свідчить про наявність в програмі поліморфного вірусу. Даний метод дозволить з великою імовірністю виявити нові поліморфні віруси.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Подловченко Р. И., Кузюрин Н. И., Щербина В. С., Захаров В. А. Использование алгебраических моделей программ для обнаружения метаморфного вредоносного кода // Труды IX Межд. конф. "Интелектуальные системы и компьютерные науки".— Москва, 2006.— Ч. 3.— С 181—199.

2. Бабанин Д. В. Модели оценки структурных решений по защите компьютерных сетей от вирусных атак // Автореф. дис. … к.т.н.— Московский государственный институт электроники и математики.— Москва, 2012.

3. Компьютерные вирусы. Программа-полифаг Aidstest [Електронній ресурс] / Режим доступу http://ref.rushkolnik.ru/v47934 (дата звернення 15.01.2013)

4. Лучший антивирус – Тесты антивирусов [Електронній ресурс] / Режим доступу http://www.anti-malware.ru/proactive_test_2010 (дата звернення 12.01.2013)

5. Jean-Maries Borello and Ludovic Me, "Code Obfuscation Techniques for Metamorphic Viruses", Feb 2008, http://www.springerlink.com/content/233883w3r2652537/

6. Гордон Я. Компьютерные вирусы без секретов.— Моква: Новый издательский дом, 2004.— С. 138—142.

O. S. Savenko, A. O. Nicheporuk

Research methods for finding polymorphic code.

This paper investigates methods for diagnosing computer systems for the presence of polymorphic viruses. The principles of operation of polymorphic viruses are considered, as well as methods for their detection. The current state of anti-virus tools is analyzed and their advantages and disadvantages are highlighted.

Keywords: *polymorphic viruses, obfuscation, signature.*