УДК 004.92

О.С. Савенко, к.т.н., доцент Хмельницького національного університету
С.М. Лисенко, к.т.н., доцент Хмельницького національного університету
А.О. Нічепорук, асистент Хмельницького національного університету

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДІАГНОСТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ НА НАЯВНІСТЬ ПОЛІМОРФНОГО ПРОГРАМНОГО КОДУ

На сьогодні розповсюдження комп'ютерних систем у всіх сферах життя є передумовою розповсюдження вірусних програм, основним завданням яких є крадіжка персональних даних, розповсюдження спаму, блокування доступу до комп'ютерної системи, завантаження інших шкідливих програм. Одним із різновидів таких програм єполіморфні віруси.Виявлення такого типу вірусів є складним завданням, у зв'язку з використанням ними техніки обфускації програмного коду. Класичні методи з використанням сигнатурного аналізу не здатні в повному обсязі виявити сучасні поліморфні віруси[1,2]. Тому, з метою підвищення достовірності та ефективності виявлення, розроблено нову інформаційну технологію діагностування комп'ютерних систем на наявність поліморфного програмного коду.

Інформаційна технологія побудована на основі моделей функціонування поліморфних вірусів [1] та використовує метод виявлення поліморфних вірусів на основі модифікованих емуляторів в корпоративній мережі [2].

Запропонований метод передбачає використанняемуляції виконання підозрілого файлу на кожному хості в мережі. З метою пошуку схожості поліморфних розшифровувачів метод передбачає залучення модифікованих емуляторів.

Хости представляють собою мережні станції для обробки інформації, що поєднанні у локальну мережу. Основними функціями хостів є здійснення одноразової емуляції виконання невідомої програми та відправлення результатів на серверну частину.

Серверна частина слугує для опрацювання результатів виконання процесу емуляції, отриманих з хостів. З метою ускладнення процесу реверс інжинірингу та захисту даних від копірайту на рівні алгоритмів реалізації, процес обфускації часто використовується у довірених додатках розробниками програмного забезпечення. Тому, основним завданням серверної частини, є класифікація отриманих з хостів векторів ознак порівняння копій метаморфних вірусів.

На стадії порівняння відбувається зіставлення програми до емуляції з цією ж програмою після виконання емуляції та формування вектора ознак схожості копій поліморфних вірусів. Процес порівняння полягає в розбитті розшифровувачів двох версій програми на функціональні блоки та поблочне їх порівняння їх за допомогою метрики Дамерау-Левенштейна.

Отримані вектори з кожного хоста відправляються на серверну частину, де відбувається формування висновку про приналежність підозрілої програми до одного із рівнів поліморфних вірусів на основі їх моделей подібності з використанням нечіткої класифікації.

Розроблена інформаційна технологіядозволяє: здійснювати виявлення поліморфних вірусів в корпоративній мережі, здійснювати класифікацію виявлених поліморфних вірусів на основі моделей поведінки поліморфних вірусів.

Список використаної літератури

1. Pomorova O. A techniquefordetectionofbotswhichareusingpolymorphiccode / O. Pomorova, O. Savenko, S. Lysenko, A. Kryshchukand A. Nicheporuk // Proceedings 21st InternationalConference, CN, Springer, Brunów, Poland, 2014, pp. 265-276
2. Савенко О.С. Метод виявлення поліморфних вірусів на основі модифікованих емуляторів / О.С. Савенко, С.М. Лисенко, А.О. Нічепорук. – Радіоелектронні і комп'ютерні системи – Харків: НАУ "ХАІ", № 6, 2016. – 35-40.