УДК 004.92

О.С. Савенко, А.О. Нічепорук (Хмельницький)

МЕТОД ВЗАЄМОДІЇ КОМПОНЕНТІВ РОЗПОДІЛЕНОЇ СИСТЕМИ ВИЯВЛЕННЯ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖАХ

Зі стрімким поширенням комп'ютерних систем та інформаційних технологій в різних галузях та сферах, а також їх інтеграція у глобальну мережу Internet, зростає кількість зловмисного програмного забезпечення, яке є одним із основних видів кіберзлочинності.

На сьогодні зловмисне програмне забезпечення (ЗПЗ) представляє собою складні багатофункційні програмні системи та комплекси, які побудовані з використанням ефективних методів протидії антивірусним системам, створення програмних засобів та поширення зловмисного коду. При цьому воно переважно націлене на використання в комп'ютерних мережах. Для організації ефективної протидії таким засобам важливим є розробка таких систем виявлення ЗПЗ, архітектура яких враховувала б ці особливості. Крім того, підвищення достовірності виявлення ЗПЗ в межах тільки однієї комп'ютерної системи (КС), яка має вихід в мережу Internet, може бути недостатнім при протидії засобам ЗПЗ, які представлені потужним програмним комплексом, що розміщений в багатьох комп'ютерних системах в глобальній мережі, і компоненти якого комунікують між собою. Проведений аналіз показав, що для виявлення ЗПЗ відомі системи здійснюють аналіз мережного трафіку, файлів аудиту, пакетів, що передаються по мережі, перевіряють конфігурацію відкритих мережевих сервісів. Для встановлення факту порушення роботи КС, використовуються різні методи машинного навчання, а саме нейронні мережі, штучні імунні системи, метод опорних векторів, Байєсові мережі, нечітку кластеризацію. Разом з тим, основним недоліком відомих систем є їх хост-орієнтований підхід [1] до виявлення ЗПЗ. Авторами розроблено удосконалені системи виявлення ЗПЗ, а також засоби їх підтримки.

Використання розробленої розподіленої системи передбачено в локальній обчислювальній мережі. Її завданнями є виявлення такого зловмисного програмного забезпечення: файлових вірусів, програмних закладок (експлоїтів), ботнет.

Розроблена архітектура [2] розподіленої системи базується на принципах децентралізації та самоорганізації і дозволяє здійснювати її наповнення різними функціоналами виявлення зловмисного програмного забезпечення в локальних обчислювальних мережах. Розподілена система відноситься до реагуючих систем, яка постійно здійснюватиме моніторинг запущених процесів та виконуваних програм в комп'ютерних системах мережі. Об'єктами для дослідження зі сторони системи є перевірка наявного програмного забезпечення та запущених процесів в комп'ютерних системах локальної мережі на можливість віднесення до зловмисного програмного забезпечення. Основою архітектури розподіленої системи виступають автономні програмні модулі з однаковими архітектурами, але при цьому кожен з них може самостійно примати рішення на основі різних даних зібраних з різних комп'ютерних систем мережі. Усі автономні програмні модулі у системі є структурно ідентичними та складаються з набору підмодулів, кожен з яких виконує певну задачу.

Для ефективної роботи системи розроблено метод взаємодії та узгодження роботи різних програмних модулів між собою на їх відповідних рівнях.

Напрямком подальших досліджень є розробка нових моделей ЗПЗ, деталізація структури розподіленої системи, її станів та наповнення підсистемами виявлення різних типів зловмисного програмного забезпечення.

Список використаної літератури

1. Lysenko S. Information technology for botnets detection based on their behaviour in the corporate area network/ S. Lysenko, O. Savenko, K.Bobrovnikova,A. Kryshchuk and B. Savenko // Communications in Computer and Information Science. – 2017. – Vol. 718. – P.167-181

2. Савенко О.С. Модель та архітектура розподіленої багаторівневої системи виявлення шкідливого програмного забезпечення в локальних комп'ютерних мережах / О.С. Савенко– Вісник Хмельницького національного університету. Серія: Технічні науки. – 2018. – № 2(259). – С.153 - 163.