УДК 681.3:519.872

В.А. Козачок, А.А. Рой, Л.В. Бурячок

ТЕХНОЛОГІЇ ПРОТИДІЇ ШКІДЛИВИМ ПРОГРАМАМ ТА ЗАВІДОМА ФАЛЬШИВОМУ ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННЮ

В статті розглянуті особливості технології протидії шкідливим програмам та завідомо фальшивому програмному забезпеченню. Обгрунтована необхідність створення систем захисту від шкідливого програмного забезпечення в інформаційних системах. Розглянуті сучасні засоби захисту від шкідливих програм. Реалізована та досліджена загальна методологія формування системи детектування на базі застосування методів виділення значимих ознак і методів класифікації шкідливого програмного забезпечення в сучасних інформаційно-телекомунікаційних системах. Показана необхідність використання прогресивних та перспективних технологій інформаційної безпеки.

Ключові слова: Захист інформації, шкідливе програмне забезпечення, виявлення шкідливого програмного забезпечення, інтелектуальний аналіз даних, методи статичного аналізу.

Постановка проблеми.

Проблема протидії шкідливому програмному забезпеченню (ПЗ), залишається досить гострою, незважаючи на появу більш ефективних механізмів його виявлення, аналізу, оновлення баз його описів і правил виявлення. Важливим аспектом цієї проблеми є пошук евристичних методів детектування, що мають більшу точність виявлення. Описуваний підхід відрізняється від існуючих спрямованістю на обробку статичної інформації, що забезпечує формування окремих функціональних елементів ефективної моделі детектування шкідливих виконуваних об'єктів. В статті реалізована та досліджена загальна методологія формування системи детектування на базі застосування методів виділення значимих ознак і методів класифікації.

Аналіз останніх досліджень та публікацій. В даний час в теорії та практиці інформаційної безпеки склалися два принципово різних напрямки реалізації способів протидії шкідливим програмам, перше з яких ґрунтується на концепції структурно-незалежних механізмів захисту інформації і припускає незалежність інформаційних процесів і процесів протидії таким програмам [1-4], а друге, що ґрунтується на концепції структурно-залежних механізмів захисту інформації, що передбачає залежність цих процесів [5-7].

Метою статті є розробка методології формування системи детектування на базі застосування методів виділення значимих ознак і методів класифікації шкідливого програмного забезпечення.

Виклад основного матеріалу.

Згідно з першим напрямком засоби протидії шкідливим програмам і ПЗ захищених інформаційних систем проектуються та розробляються незалежно один від одного, причому засоби протидії шкідливим програмам додаються до вже розробленого ПЗ.

Особливістю механізму протидії в цьому випадку є те, що функції виявлення шкідливих програм реалізуються шляхом періодичного контролю цілісності обчислювального середовища захищених інформаційних систем з метою реєстрації несанкціонованих змін, викликаних шкідливими програмами.

Згідно з другим напрямом реалізується дворівнева система ідентифікації впливів шкідливих програм ідентифікація факту впливу і ідентифікація слідів впливу. У свою чергу, ідентифікація факту дії шкідливої програми представляється дворівневим механізмом контролю процесів функціонування захищеної інформаційної системи, що реєструє її некоректну поведінку, а саме:

- шляхом порівняння поточних результатів виконання функцій обробки інформації та функцій контролю, отриманих в динаміці функціонування;
- шляхом виконання операцій порівняння поточних параметрів обчислювального процесу в захищеної інформаційної системи з наперед відомими еталонними величинами.

Особливістю такої сукупності засобів контролю є те, що кожний такий засіб окремо володіє обмеженими контрольними характеристиками шкідливих функцій, так як може охопити лише деякі, в основному не явні ознаки і прояви шкідливих програм. Для правильного прийняття рішення про те, що некоректне функціонування захищеної інформаційної системи зумовлене саме впливом шкідливих програм, проводиться аналіз усієї сукупності сформованих в результаті ідентифікації фактів впливу значущих ознак такого функціонування (трасологія впливу). При цьому аналізується послідовність всіх контрольних точок і викликів елементів у відповідності з ієрархією його побудови з метою отримання інформації про час, місце та умови прояву впливу шкідливої програми та наслідків такого впливу.

В основу реалізації структурно-незалежних механізмів ідентифікації шкідливих програм в захищених інформаційних системах покладені способи їх детектування за допомогою професійних пакетів антивірусних засобів. Основними методами при цьому є:

- сканування;
- евристичне сканування;
- CRC-сканування;
- антивірусний моніторинг;
- імунізація.

Принцип роботи антивірусних сканерів заснований на перевірці файлів, секторів і системної пам'яті, а також пошуку в них відомих і нових вірусів. Для пошуку відомих вірусів використовуються так звані «сигнатури» – послідовності байтів, однозначно характерні для конкретного вірусу. Довжина сигнатури повинна бути як можна більше, а в ідеалі – в сигнатуру повинна входити вся незмінна частина вірусу, що гарантує однозначність ідентифікації. Разом з тим це б значно збільшило обсяг антивірусу і суттєво уповільнило процес сканування. Як правило, доцільною вважається довжина сигнатури від одиниць байт до десятків байт, але не більше.

Сканери поділяються на резидентні, що виробляють постійне сканування в ре - жимі реального часу, і не резидентні, що забезпечують перевірку системи тільки за запитом. Як правило, резидентні сканери забезпечують більш надійний захист системи, оскільки вони негайно реагують на появу вірусу, в той час як нерезидентний сканер здатний розпізнати вірус лише під час свого чергового запуску. До переваг сканерів всіх типів відноситься їх універсальність, до недоліків – розміри антивірусних баз, які сканерам доводиться включати в себе, і відносно невелику швидкість пошуку вірусів.

Використовуються у багатьох антивірусних пакетах алгоритми аналізу послідовності команд з метою формування деякої статистики та прийняття рішень про можливість зараження для кожного об'єкта, що перевіряється, які у відомій літературі [5] получили назву методів евристичного сканування. Універсальність методів евристичного сканування дозволяє детектувати велику кількість шкідливих програм. Оскільки евристичне сканування є багато в чому імовірнісним методом пошуку шкідливих програм, то на нього поширюються багато законів теорії ймовірностей. Наприклад, чим вище відсоток виявлення вірусів, тим більше кількість помилкових спрацьовувань. Недоліком методів евристичного сканування є відносно невисока швидкість пошуку шкідливих програм. Слід зауважити, що останнім часом спостерігається тенденція застосування евристичних сканерів так званих антивірусних баз, де зберігається інформація про характерні фрагменти кодів шкідливих програм та дозволяє лише підвищити можливості виявлення таких програм, у той час як швидкість їх пошуку практично не збільшується.

Деякі антивірусні засоби для виявлення шкідливих програм, що реалізують алгоритми, засновані на підрахунку контрольних сум (CRC-сум) для всіх збережених на носіях файлів і системних секторів. Інформація про контрольні суми, дані про довжину файлів, а також дані їх останньої модифікації і т. ін. зводиться в базу даних і використовується при наступних запусках CRC-сканерів для порівняння із реально підрахованими значеннями. Якщо інформація про файл, записана у базі даних, не збігається з реальними значеннями, то CRC-

сканери сигналізують про вплив шкідливої програми. Аналіз алгоритмів CRC-сканування показує, що найкращі можливості по виявленню шкідливих програм мають CRC-сканери, що використовують так звані «антистелс»-алгоритми. Однак у цього типу антивірусів є принциповий недолік, який полягає в тому, що CRC-сканери не здатні виявити шкідливу програму в момент її появи в системі, а роблять це лише через деякий час, вже після того, як шкідлива програма стала реалізовувати свої функції. CRC-сканери не можуть детектувати шкідливу програму у нових файлах, наприклад, в електронній пошті, на дискетах, у файлах, відновлюваних з файлів типу «backup» або при розпакуванні файлів з архіву, оскільки в їх базах даних відсутня інформація про ці файли. Більше того, періодично з'являються шкідливі програми, які використовують цю «слабкість» CRC-сканерів, заражають тільки новостворювані файли і залишаються, таким чином, невидимими для CRC-сканерів.

Антивірусні монітори – це резидентні програми, контролюючі виникнення ситуацій, пов'язаних з функціонуванням шкідливих програм. До таких ситуацій відносяться виклики на відкриття для запису у виконувані файли, запис у завантажувальні сектори дисків або вінчестера, спроби програм залишитися резидентними і т. ін., тобто виклики, які характерні для програм вірусного типу. До переваг моніторів належить їх здатність виявляти і блокувати шкідливі програми на самій ранній стадії їх прояви. До недоліків відноситься велика кількість помилкових спрацьовувань, що, мабуть, і стало причиною непопулярності такого роду антивірусних програм серед користувачів.

Останнім часом, завдяки своїй надійності, з'явилися антивірусні монітори, виконані у вигляді апаратних компонентів комп'ютера. Найбільш поширеною є вбудований в BIOS захист від запису. Разом з тим, складність настройки і вимоги апаратної сумісності таких типів моніторів серйозно стримує їх застосування. Імунізатори – це програми, що імітують зараження файлів шкідливими програмами. Імунізатори діляться на два типи:

- імунізатори, які здійснюють контроль власного тіла;
- імунізатори, які блокують зараження певним типом шкідливої програми.

Перші зазвичай записуються в кінець файлів (за принципом файлового вірусу) і при запуску файлу кожен раз перевіряють його на зміну. Недоліком таких імунізаторів є нездатність детектувати зараження шкідливою програмою, яка використовує «стелс»-алгоритм. Другий тип імунізації захищає елементи комп'ютерних мереж від ураження вірусом певного виду. Файли на дисках модифікуються таким чином, що вірус сприймає їх як вже заражені. Для захисту від шкідливих програм з механізмами резидентного вірусу в пам'ять комп'ютера заноситься програма, що імітує копію вірусу: при спробі шкідливої програми впровадитися в файли імунізатор повідомляє їй про те, що вже заражені файли.

Аналіз вітчизняних і зарубіжних антивірусних засобів показує, що більшість з такого роду засобів використовують декілька механізмів детектування шкідливих програм. В таблиці 1 представлені результати такого аналізу [2]. Слід зазначити, що якісне детектування в більшості випадків забезпечується більш новими антивірусними засобами, бази даних яких мають, як правило, сигнатури самих нових шкідливих програм.

Таблиця 1

Механізми детектування шкідливих програм

Найменування антивірусного засобу	Механізм				
	Сканування	Евристичне сканування	CRC сканування	Моніторинг	Імунізація
ADINF («Діалог-Наука»)			+		
DrWeb («Діалог-Наука»)		+		+	
AVP («Лабораторія Касперського»)	+			+	
Norton AntiVirus (Norton Inc.)	+			+	

McAfee SCAN	+				
Service Pack					+

Аналіз типових ситуацій впливу шкідливих програм на інформаційні процеси в захищених інформаційних системах дозволив встановити, що дії шкідливих програм, як специфічного виду резидентних комп'ютерних вірусів файлового типу формально можна представити наступною послідовністю кроків [6]:

- перехоплення управління шляхом передачі помилкового запиту базового модулю операційної системи (ОС) функцій на обслуговування переривань по виконанню програм (крок 1);
- відновлення початкового вигляду програми, в яку впроваджено шкідлива програма (крок 2);
- інфікування оперативної пам'яті комп'ютера (крок 3);
- виконання шкідливих функцій з протиправного маніпулювання інформацією (крок 4);
- повернення управління основній програмі (крок 5).

Сутність відповідних цим крокам способів ідентифікації впливів шкідливих програм полягає в такому. Найбільш доцільною формою виявлення дій шкідливих програм, відповідних кроків 1, 2 і 3, є:

1) порівняння послідовності виконуваних контрольних точок у програмі з еталонною (контрольна функція типу 1);

2) аналіз початку файлу на наявність кодів команди переходу або коду, який не відповідає реальній адресі її запуску та відноситься до типу контрольних операцій перевірки відповідності даних області значень (контрольна операція типу 1);

3) аналіз векторів переривань, відповідних функцій завантаження і виконання програм, які також відносяться до типу контрольних операцій перевірки відповідності даних області значень (контрольна операція типу 1).

Так як при виконанні даних кроків шкідлива програма реалізує системні функції, операції виявлення повинні проводитися тільки компонентами ОС під управлінням її базового модуля. При цьому еталонна послідовність контрольних точок повинна бути захищена.

Для контролю виконання шкідливих функцій доцільно використовувати як систему контрольних перевірок, контролюючих виконання окремих операцій, так і реалізацію цілих функцій ПЗ по обробці і передачі інформації в захищених інформаційних системах. При цьому перевірка операцій обробки і передачі інформації в ПЗ здійснюється операціями контролю, а перевірка функцій обробки – функціями контролю, що реалізуються окремими модулями контролю. Основними операціями контролю є:

- перевірка відповідності даних області значень (контрольна операція типу 1);
- перевірка граничних значень вхідних даних, проміжних і вихідних результатів (контрольна операція типу 2);
- перевірка часу виконання ПЗ (контрольна операція типу 3);
- перевірка періодичності видачі результатів або періодичності виконання ПЗ (контрольна операція типу 4);
- перевірка відповідності даних їх типами (контрольна операція типу 5);
- перевірка формату записів даних необхідними шаблонами (контрольна операція типу 6).

До числа основних функцій контролю належать:

- перевірка результатів шляхом обробки іншим методом (контрольна функція типу 2);
- перевірка результатів шляхом отримання від них вихідних даних зворотною обробкою (контрольна функція типу 3);
- перевірка розрахункових значень деяких ознак одержуваних результатів (кількість записів, обсяги масивів і т. ін.) з їх поточними значеннями (контрольна функція типу 4);
- перевірка поточних значень полів даних у записах і масивах шляхом порівняння результатів виконання математичних операцій над ними із заздалегідь обчисленими умовами (контрольна функція типу 5);

- перевірка поточних значень результатів обробки зі значеннями математично або логічно пов'язаних з ними величин (контрольна функція типу 6);
- перевірка смислових співвідношень між результатами обробки (контрольна функція типу 7).

Так як при виконанні цього кроку шкідлива програма реалізує прикладні функції, операції виявлення її впливу можуть проводитися компонентами прикладного ПЗ без залучення компонентів ОС.

Найбільш доцільною формою контролю дій шкідливої програми на кроці повернення управління основній програмі (крок 5) є, як і на кроці перехоплення управління (крок 1), порівняння послідовності виконуваних контрольних точок у програмі з еталонною (контрольна функція типу 1), виконуваної компонентами ОС.

Узагальнені результати розглянутого аналізу способів виявлення впливів шкідливих програм наводяться в таблиці 2 [6].

Таблиця 2

Форми та рівні контролю кроків дії шкідливих програм

Кроки дії шкідливої програми	Форма контролю	Рівень контролю
1	Контрольна функція типу 1	Системний
2	Контрольна операція типу 1	Системний
3	Контрольна операція типу 1	Системний
4	Контрольні операції типу 1-6 Контрольні функції типу 2-7	Прикладний
5	Контрольна функція типу 1	Системний

Висновок

Особливістю ідентифікації слідів впливу шкідливих програм є простеження через точки виклику програмних модулів всієї послідовності виконання інформаційного процесу у всіх контрольних точках. Самі ж контрольні точки вибираються виходячи з вимог достовірності ідентифікації фактів впливом навколишнього середовища шкідливих програм.

Список використаної літератури

1. Козлов С.Е. Теорія і практика боротьби з комп'ютерною злочинністю /В. О. Козлов. – М.: Гаряча лінія. – Телеком, 2012. — 176 с.

2. Касперски К. Техніка мережних атак. Прийоми протидії / К. Касперски. – — М.: Солон-Р, 2011. – 397с.

3. Сердюк С.А. Перспективні технології виявлення інформаційних атак/ В. А. Сердюк // Системи безпеки. – 2012. – № 5(47). – С. 96-97.

4. Антимонов Ц.Р. Інтелектуальні протистояння по лінії фронту Вірус-антивірус // Інформація і безпека: матеріали міжрегіональної науково-практ.конф. – Інформація і безпека. – Випуск 2. – Воронеж: ВДТУ, 2012. – С. 39-46.

5. Розподілений антивірусний контроль як спосіб протидії злоякісним програмами в автоматизованих інформаційних системах / С.В. Скриль та ін // Радіосистеми. – Вип. 37 «Радіотехнічні та інформаційні системи охорони і безпеки». – Радіотехніка. – 2014. – №6. – С. 27-30.

6. Мінаєв С.А. Принципи організації протидії шкідливим програмам в інформаційно-телекомунікаційних системах на основі оптимізації їх функціонування / В. А. Мінаєв, С. В. Скриль // Радіосистеми. – Вип. 47 «Радіотехнічні і інформаційні системи охорони і безпеки». – Радіотехніка. – 2013. – №9. – С. 71-72.

7. Лозинський Д.Н. Інформаційна безпека. Проблема нового тисячоліття/ Д. Н. Лозинський, Е. В. Плескач // Системи безпеки. – 2014. – № 4(46). – С. 13.

Надійшла 20.04.2017 р. Рецензент: д.т.н., проф. Єрохін В.Ф.