ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 681.3

О. П. ВОЙТОВИЧ, В. О. ВІТЮК, В. А. КАПЛУН

Вінницький національний технічний університет, м. Вінниця

ОСОБЛИВОСТІ ДОСЛІДЖЕННЯ ОЗНАК ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ БЕЗ НАЯВНОСТІ ВИХІДНИХ КОДІВ

Анотація. В статті розглянуті особливості розслідування комп'ютерних інцидентів при знаходженні в атакованій системі шкідливого програмного забезпечення. Розглянуті відомі технології виявлення ознак шкідливого програмного забезпечення. Запропонована математична модель, що описує ознаки шкідливого програмного забезпечення. Удосконалено підхід для моніторингу шкідливих функцій, який реалізовано у вигляді програмного засобу.

Ключові слова: дослідження комп'ютерних інцидентів, шкідливе програмне забезпечення, HIPS, VIPS, пісочниця, узагальнена математична модель виявлення ознак шкідливого програмного забезпечення

Аннотация. В статье рассмотрены особенности расследования компьютерных инцидентов при нахождении в атакованной системе вредоносных программ. Рассмотрены известные технологии обнаружения признаков вредоносного программного обеспечения. Предложена математическая модель, описывающая признаки вредоносного программного обеспечения. Усовершенствован подход для мониторинга вредоносных функций, который реализован в виде программного средства.

Ключевые слова: исследования компьютерных инцидентов, вредоносное программное обеспечение, HIPS, VIPS, песочница, обобщенная математическая модель выявления признаков вредоносного программного обеспечения

Abstract. The peculiarities of computer incidents investigating in the system attacked by malware were considered. Known technologies of detecting malicious software are investigated. A mathematical model that describes the malware characteristics is described. Improved approach for detecting malware functions is implemented as software.

Key words: researching of computer incidents, malware, HIPS, VIPS, sandbox, mathematical model of malware detecting

Вступ

З перенесенням основних бізнес-процесів підприємств в інформаційно-комунікаційні системи все частіше трапляються випадки компрометації окремих систем. Причому, методи та шляхи атак стають все більш різноманітними, часто зловмисники впроваджують своє програмне забезпечення (ПЗ) для використання систем як «зомбі» для атак на інші системи та персональні комп'ютери [1].

Актуальність

Шкідливе ПЗ може проникнути до комп'ютерної системи через недостатнє дотримання політики безпеки з боку користувачів, наприклад через встановлення недовіреного ПЗ, або в результаті реалізації атаки зловмисником. При дослідженні комп'ютерних інцидентів недостатньо лише виявити, що певне ПЗ містить шкідливі (недокументовані) функції, необхідно знати, які саме процеси виконувались в операційній системі (ОС). Наприклад, яка інформація перехоплювалась, до яких файлів чи програм здобувався доступ, який мережевий порт відкривався для доступу тощо. Стандартні антивірусні системи зазвичай дають інформацію лише про назву та основні характеристики шкідливого ПЗ, не вказуючи необхідних для дослідника відомостей [2]. При цьому стоїть задача дослідження ПЗ без наявності вихідних кодів, що значно ускладнює роботу дослідника [1]. Основні ознаки наявності недокументованих функцій такі: запис у реєстр (особливо зміна гілок реєстру, що стосуються системних або інших програм), доступ на читання/запис до файлів та оперативної пам'яті, доступ до периферійних пристроїв, мережева активність, звертання до поштових систем, відправлення повідомлень, зміна налаштувань програм, зокрема інтернет-браузерів, звертання до тимчасових файлів інших програм, пошук за сигнатурами, перехоплення переривань та системних функцій тощо [3,4].

Мета

При досліджені комп'ютерних інцидентів часто постає питання виявлення не тільки факту наявності шкідливого ПЗ, але й визначення, які саме функції виконувались. Метою даної статті є дослідження та розробка технологій, які дозволяють покращити виявлення ознак шкідливого ПЗ.

Аналіз проявів та ознак шкідливого ПЗ

Під терміном шкідливе ПЗ розуміють програмні засоби, що несанкціоновано впроваджуються у комп'ютерну систему, і, які здатні викликати порушення політики безпеки, завдавати шкоди інформаційним ресурсам, а в окремих випадках, й апаратним ресурсам комп'ютерної системи [3].

Найпопулярнішими видами шкідливого ПЗ є такі [5,6]: комп'ютерний вірус – різновид шкідливих програм, метою яких є проведення дій, що завдають шкоди власникові комп'ютерній системі. Відмінною особливістю вірусів є здатність до розмноження та впроваджуватись в тіло програм, завантажувального сектору, документа тощо; троянська програма – шкідлива програма, яка проникає на комп'ютер жертви під виглядом нешкідливої (наприклад, кодек, системне оновлення, заставки, драйвера тощо); мережевий черв'як – самостійна шкідлива програма, яка проникає на комп'ютер жертви, використовуючи

уразливості в ПЗ операційних систем; руткіт – програма, призначена для приховування слідів шкідливих дій зловмисника в системі.

Різні типи шкідливого ПЗ у комп’ютерній системі поводять себе по-різному, але можна виділити наступні ознаки, що найчастіше помічають користувачі комп’ютерних систем: виведення на екран неочікуваних повідомлень або зображень; подача непередбачених звукових сигналів; довільний запуск на комп'ютерних програм без виклику користувача; поява попереджень від міжмережевого екрану про спробу програми вийти в Інтернет; відправлення листів через електронну пошту на адреси, які збережені в контактах; у поштовій скриньці знаходиться велика кількість повідомлень без зворотної адреси і заголовка.

Якщо користувач помічає, що з комп'ютером відбувається подібне, то з великою мірою вірогідності можна передбачити, що комп'ютер заражений шкідливим ПЗ.

Крім даних ознак існують непрямі ознаки зараження комп'ютера: часті зависання і збої в роботі комп'ютера; повільна робота комп'ютера при запуску програм; неможливість завантаження операційної системи; зникнення файлів і каталогів або спотворення їх вмісту; часте звернення до жорсткого диска (часто блимає лампочка на системному блоці); інтернет-браузер «зависає» або поводиться несподіваним чином (наприклад, вікно програми неможливо закрити).

За цими ознаками, які може помітити користувач відбуваються операції, дані про які можна отримати лише спеціалізованими засобами. А саме дані про:

- читання/запис даних у файловій системі – створення, видалення, редагування файлів, каталогів, дописування інформації в файл;
- модифікації пам'яті – створення чи завершення процесів, створення прихованих процесів;
- зміни реєстру – створення нових записів в реєстрі, редагування або видалення існуючих;
- зовнішня мережева активність – отримання чи відсилання інформації через мережу;
- внутрішня мережева активність - отримання чи відсилання інформації через localhost;
- перехоплення хуків клавіатури;
- відкриття портів;
- запуск файлів в операційній системі;
- встановлення чи заміна драйверів.

Отже, для виявлення ознак шкідливого ПЗ, його потрібно досліджувати за наведеними вище параметрами.

Аналіз існуючих технологій виявлення ознак шкідливого ПЗ

На сучасному етапі розвитку систем захисту ПЗ серед програм, які включають компоненти виявлення ознак шкідливого ПЗ, найпопулярнішими є такі: ThreatExpert [7], Process Monitor[8], Defense Wall HIPS[9], SafenSoft SysWatch Deluxe [10] та деякі інші. Вони використовують один з трьох основних методів контролю активності ПЗ: HIPS, VIPS та Пісочниця (sandbox).

Технологія HIPS – це технологія контролю активності, заснована на перехопленні звернень до ядра ОС і блокуванні виконання потенційно небезпечних дій ПЗ, яке працює в режимі користувача, виконуваних без відома користувача [5]. За допомогою власного драйвера перехоплює всі звернення ПЗ до ядра ОС. У разі спроби виконання потенційно небезпечного дії з боку ПЗ, HIPS-система блокує виконання даної дії і видає запит користувачеві, який вирішує дозволити або заборонити виконання даної дії. Схема взаємодії процесів і ядра ОС в методі HIPS показано на рис. 1.

Переваги систем, побудованих на методі HIPS:

- низьке споживання системних ресурсів;
- не вимогливі до апаратного забезпечення ПК (можуть працювати на різних платформах);
- можливість визначення загроз нульового дня;
- можливість визначення руткітів, які працюють в режимі користувача.

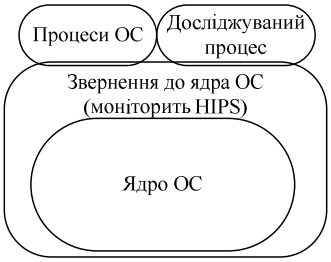

Рисунок 1 - Схема взаємодії процесів і ядра ОС в технології HIPS

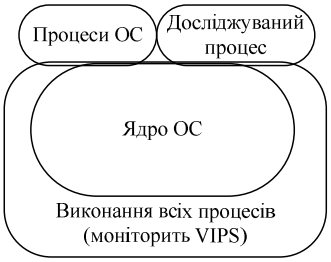

Рисунок 2 - Схема взаємодії процесів і ядра ОС в технології VIPS

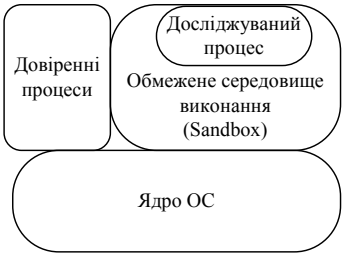

Рисунок 3 - Схема взаємодії процесів і ядра ОС в технології пісочниця