УДК 004.056.57

Вадим Іванович Пеньков
Роман Михайлович Штонда
Олександр Миколайович Гук
Ірина Робертівна Мальцева
Юлія Олександрівна Черниш

Військовий інститут телекомунікацій та інформатизації, Київ, Україна

МЕТОДИ ТА ЗАСОБИ ПРОТИДІЇ ШКІДЛИВОМУ ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННЮ

Інформаційні технології визначають процеси передачі, зберігання та обробки інформації, а також її використання в певних цілях. Ці процеси повинні бути швидкими, найменш витратними, максимально корисними, зручними і автоматизованими. З цієї причини основною тенденцією розвитку інформаційних технологій є їх подання в цифровому вигляді, перехід до цифрових інформаційно-телекомунікаційних баз, заснованим на цифровій взаємодії комп'ютерів, розроблених з найрізноманітнішими функціональними алгоритмами. Впровадження персональних комп'ютерів в інформаційну сферу й застосування телекомунікаційних засобів зв'язку визначили новий етап розвитку інформаційних технологій.

Розвиток Інтернету змінив ставлення до проблем безпеки, піднявши питання про захищеність локальних і глобальних комп'ютерних мереж. Ще донедавна ці проблеми не були актуальними. Розробники перших комп'ютерних мереж в першу чергу прагнули збільшити швидкість і надійність передачі даних, часом досягаючи бажаного результату на шкоду безпеці.

Збільшення швидкості передачі інформації, обсягів і значимості оброблюваних в обчислювальних мережах даних відкриває перед кіберзлочинцями все більш широкі можливості. Поширення по всьому світу шкідливого програмного забезпечення займає лічені дні або навіть години. Сотні мегабайт оперативної пам'яті дозволяють виконувати практично будь-які дії непомітно для користувача. Спектр можливих цілей, таких як паролі, карткові рахунки, ресурси віддалених комп'ютерів представляє величезне поле для діяльності.

Ключові слова: *шкідливе програмне забезпечення, антивірусні програми, комп'ютерний вірус, комп'ютерна система, комп'ютерна мережа.*

Вступ

Шкідливі програми і боротьба з наслідками їх діяльності протягом останнього десятиріччя є однією з найсерйозніших проблем для всіх, хто працює за комп'ютером, від IT-директорів до домашніх користувачів. Постійне оновлення антивірусних програмних засобів – невід'ємний атрибут будь-якої корпоративної мережі, серверів Інтернет-провайдерів і значної частини особистих комп'ютерів. Останнім часом користувачі Інтернет все частіше відчувають потребу в отриманні подібних засобів або безпосередньо у складі операційних систем і серверних продуктів, або у вигляді додаткових послуг від постачальників зазначених категорій програмних засобів.

Постановка проблеми. За створення, використання і розповсюдження шкідливих програм передбачена відповідальність, у тому числі і кримінальна, в законодавстві багатьох країн світу.

У Кримінальному Кодексі України термін "шкідливий програмний засіб" детально не визначений. Але попри це Стаття 361-1 КК України передбачає покарання за "Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку."

Критерії, за якими програмні продукти можуть бути віднесені до категорії "шкідливих програмних засобів" досі ніде чітко не обумовлені. Відповідно, для того, щоб твердження про шкідливість програмного засобу мало юридичну силу, необхідно провести програмно-технічну експертизу з дотриманням всіх встановлених чинним законодавством формальностей.

Аналіз останніх досліджень і публікацій. Проблемам виявлення шкідливих програмних засобів та захисту від них присвячено ряд робіт, серед яких треба виділити праці Безрукова М. [1], Гульєва І. [2], Козлова Д.А. [3], Собейкіса В.Г. [4], Шаньгіна В. [5] та інших. В цих працях здебільшого розкриваються напрямки, методи та засоби протидії шкідливим програмам.

Метою статті є визначення методів та засобів захисту комп'ютерних систем від

шкідливих програмних засобів.

Виклад основного матеріалу дослідження

В даний час в теорії і практиці інформаційної безпеки склалися два принципово різних напрямки реалізації способів протидії шкідливим програмам.

Перший напрямок заснований на концепції структурно незалежних механізмів захисту інформації і припускає незалежність інформаційних процесів, і процесів протидії таким програмам. В цьому напрямку засоби протидії шкідливим програмам та програмному забезпеченню захищених інформаційних систем проектуються і розробляються незалежно один від одного, причому засоби протидії шкідливим програмам придані до вже розроблених програмних засобів. 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.

Другий напрямок заснований на концепції структурно-залежних механізмів захисту інформації і передбачає залежність цих процесів. Згідно з цим напрямом реалізується дворівнева система ідентифікації впливів шкідливих програм: ідентифікація факту впливу та ідентифікація слідів впливу. У свою чергу, ідентифікація факту впливу шкідливої програми представляється дворівневим механізмом контролю процесів функціонування захищеної інформаційної системи, реєструючи некоректну поведінку її програмних засобів:

шляхом порівняння поточних результатів виконання функцій обробки інформації та функцій контролю, отриманих в динаміці функціонування програмних засобів;

шляхом виконання операцій порівняння поточних параметрів обчислювального процесу в захищеній інформаційній системі із заздалегідь відомими еталонними величинами.

Особливістю такої сукупності засобів контролю є те, що кожен такий засіб окремо має обмежені контролюючими характеристиками шкідливі функції, так як може охопити лише деякі, в основному неявні, ознаки та прояви шкідливих програм. Для правильного прийняття рішення проводиться аналіз некоректного функціонування програмних засобів захищеної інформаційної системи. В результаті формуються ідентифікації фактів впливу значущих ознак такого функціонування (трасологія впливу). При цьому аналізується послідовність всіх контрольних точок і викликів елементів програмних засобів відповідно до ієрархії їх побудови, з метою отримання інформації про час, місце та умови прояву впливу шкідливої програми та наслідків такого впливу.

Однак, у більшості випадків, наявність встановленої антивірусної програми, може виявитися недостатнім для повноцінного захисту. Як показано на рис. 1 один антивірусний засіб не завжди може гарантувати стовідсотковий захист від шкідливих програм [6].

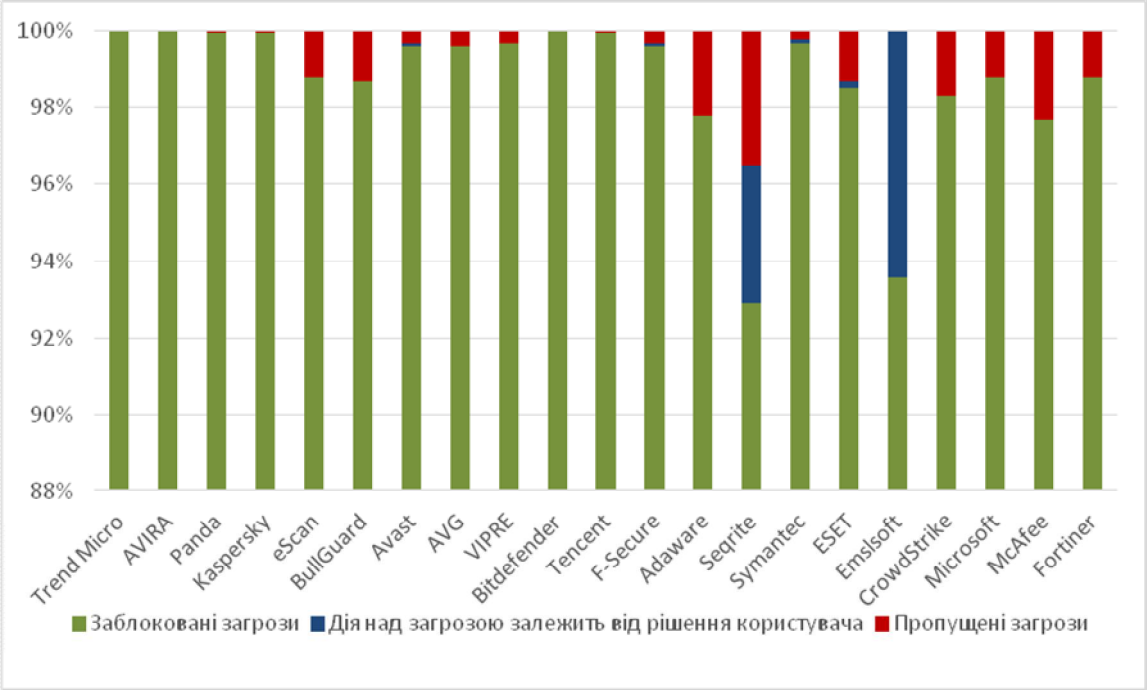


Рис. 1. Тест антивірусних засобів на захист від шкідливих програм

Тому в більшості випадків потрібно використовувати додаткові методи та способи.

Зазвичай через неправильне використання антивірусних програм, ігнорування порад щодо їх встановлення та самої роботи виробника антивірусних програм, методи та способи захисту можна розділити на три типи: правові, організаційні та технічні.

Правові методи зводяться до встановлення відповідальності за створення і поширення шкідливих програм, і заподіяння збитку. Слід зазначити, що довести авторство і умисність створення таких програм досить важко.

Організаційний захист полягає у виробленні та неухильному здійсненні заходів, спрямованих на попередження проникнення шкідливих програм в інформаційні системи, виявлення зараження, нейтралізацію негативного впливу і ліквідацію наслідків.

Технічні методи спрямовані на зміни в комп'ютерній системі, і полягають у використанні додаткових засобів захисту, які розширюють і доповнюють можливості антивірусних програм.

Такими засобами захисту можуть бути:

брандмауери-програми, що захищають від атак по мережі;

засоби боротьби зі спамом;

виправлення, що усувають "дірки" в операційній системі, через які можуть проникати віруси;

інші різні спеціальні утиліти для дослідження системи.

Крім того, можуть використовуватися спеціальні пристрої, що перешкоджають проникненню шкідливих програм на комп'ютер, пристрої резервного копіювання даних і так далі.

Технології, що використовуються в антивірусних програмах, можна розбити на дві групи:

технології сигнатурного аналізу;

технології імовірнісного аналізу.

Найпершою технологією пошуку шкідливих програм був сигнатурний аналіз.

Сигнатурний аналіз – метод виявлення вірусів, що полягає в перевірці наявності в ділянках коду сигнатур вірусів [5]. Сигнатурний аналіз є найбільш відомим методом виявлення вірусів і використовується практично у всіх сучасних антивірусних програмах.

Сам принцип роботи сигнатурного аналізу також визначає межі його функціональності – можливість виявляти лише вже відомі віруси, проти нових вірусів сигнатурний сканер безсилий, тому бази сигнатур необхідно оновлювати регулярно.

Грамотна реалізація вірусної сигнатури дозволяє виявляти відомі віруси зі стовідсотковою ймовірністю

В той час як еволюціонували віруси, ускладнювалися і розвивалися технології їх детектування.

Технології імовірнісного аналізу (несигнатурні технології) в свою чергу можна розбити на три категорії:

евристичний аналіз – технологія, заснована на імовірнісних алгоритмах, результатом роботи яких є виявлення підозрілих об'єктів. У процесі евристичного аналізу перевіряється структура файлу, його відповідність вірусним шаблонам. Найбільш популярною евристичною технологією є перевірка вмісту файлу на предмет наявності модифікацій уже відомих сигнатур вірусів та їх комбінацій. Евристичний аналіз застосовується для виявлення невідомих вірусів, і, як наслідок, не передбачає лікування;

поведінковий аналіз – технологія, в якій рішення про характер об'єкта, що перевіряється приймається на основі аналізу операцій, які ним виконуються. Поведінковий аналіз нечасто застосовується на практиці, оскільки більшість дій, характерних для вірусів, можуть виконуватися і звичайними додатками. Поведінкові аналізатори не використовують для роботи додаткових об'єктів, подібних вірусних баз і, як наслідок, нездатні розрізняти відомі й невідомі віруси - всі підозрілі програми апріорі вважаються невідомими вірусами;

аналіз контрольних сум – це спосіб відстеження змін в об'єктах комп'ютерної системи. На підставі аналізу характеру змін – одночасність, масовість, ідентичність змін довжин файлів – можна зробити висновок про зараження системи. Подібні технології застосовуються в сканерах при першій перевірці з файлу знімається контрольна сума і розміщується в кеші, перед наступною перевіркою того ж файлу сума знімається ще раз, порівнюється, і в разі відсутності змін файл вважається незараженим.

Поза всяким сумнівом, головною зброєю в боротьбі з вірусами завжди були антивірусні програми. Вони дозволяють не тільки виявляти віруси, що використовують різні методи маскування, але і видаляти їх з комп'ютера. Розрізняють наступні види антивірусних програм: вакцини; детектори; ревізори; охоронці; монітори; поліфаги; евристичні аналізатори.

Останнім часом, розробники антивірусних програм, пропонують користувачам комплексні рішення, які включають в себе більшу частину або навіть всі вищевказані програми.

Вакцини – це програми, призначені для запобігання зараження файлів від якого-небудь одного, конкретного вірусу. Вакцини застосовуються, якщо відсутні програми, що можуть знешкодити даний вірус. Вакцинація можлива тільки від відомих вірусів, які можна виявити, але неможливо знешкодити. Програма-вакцина модифікує програму, яка захищає комп'ютерну систему таким чином, щоб це не відображалося на її роботі, але при цьому справжній вірус вважав цю програму зараженою. Дії програм-вакцин засновані на одній з базових властивостей комп'ютерних вірусів – не заражати повторно вже інфіковану програму. З цією метою, при зараженні програм, віруси використовують так звану "чорну мітку", яка б дозволяла відрізняти вже інфіковані програми від неінфікованих. Це може бути, наприклад установка часу створення файлу в 24 години 1 хвилину і 62 секунди. Так як нормальні програми не можуть мати подібного часу створення, то, виявивши, що файл створений в цей час, вірус вважає, що він заражений і не намагається інфікувати його повторно.

Таким чином, програма-вакцина просто створює "чорну мітку" конкретного вірусу в програмі, що захищає не змінюючи її виконуваного коду, а вірус, виявляючи таку мітку, уже не намагається заразити даний файл.

"Детектори" або "сканери" – це програми, які здійснюють пошук характерної для конкретного вірусу сигнатури, в оперативній пам'яті комп'ютера або в файлах на жорсткому диску, і при виявленні, видають відповідне повідомлення. Недоліком цього класу антивірусних програм є те, що вони можуть знаходити тільки ті віруси, які відомі розробникам.

"Ревізори" – це програми, які належать до найбільш надійних засобів захисту від вірусів. Заражаючи комп'ютер, вірус робить зміни на жорсткому диску: дописує свій код в заражений файл, змінює системні області диска і таке інше. На виявленні таких змін ґрунтується робота антивірусних програм ревізорів. Вони побудовані на принципі, зворотного принципу побудови сканерів. Ревізори не знають в обличчя конкретні віруси, але вони запам'ятовують інформацію про кожен конкретний логічний диск і при зміні цієї інформації, дозволяють надійно виявляти, як відомі, так і нові, невідомі віруси. У разі виявлення зміни відомостей в комп'ютерній системі, вся відповідна інформація про змінений об'єкт надається користувачеві. Він вже сам повинен прийняти рішення: чи варто, наприклад, перевіряти даний файл на вірус (якщо це виконавчий файл) або проігнорувати повідомлення, якщо файл змінювався самим користувачем. Як правило, порівняння станів проводиться відразу після завантаження операційної системи. При порівнянні перевіряються довжина файлу, його контрольна сума, дата і час модифікації, і деякі інші параметри. Програми-ревізори мають достатньо розвинуті алгоритми, що дозволяють виявляти навіть віруси таких класів як "стелс"-віруси і "поліморфні" віруси, а деякі навіть можуть відновити вихідну версію програми, що перевіряється, видаливши зміни, внесені вірусом.

Перевагою ревізорів є – висока швидкість перевірки дисків (у багато десятків разів перевищує швидкість роботи сканерів) і висока надійність виявлення навіть невідомих вірусів.

"Охоронці" – це невеликі резидентні програми, призначені для виявлення підозрілих дій, що виникають при роботі користувача на комп'ютері, і характерних для вірусів.

Одним з найбільших недоліків програм цього класу є те, що при неправильному (а іноді навіть і при правильному) налаштуванні, вони буквально "засипають" користувача попередженнями, в результаті чого їх зазвичай відключають.

"Монітори" (або програми-фільтри) – це антивірусні програми які використовують для виявлення вірусів бази даних та їх сигнатури. Антивірусний монітор розташовується резидентно в пам'яті комп'ютера, і перевіряє на наявність вірусів тільки ті програми, над якими робить будь-які маніпуляції користувач, або операційна система.

Програми-фільтри є корисними з тієї точки зору, що допомагають користувачеві виявити вірус на ранній стадії його існування, ще до того моменту, коли поширення вірусу прийме характер епідемії.

"Поліфаги" – це програми, які здатні благополучно видалити вірус і відновити працездатність зіпсованих програм.

Для кожного вірусу, шляхом аналізу його коду, способів зараження файлів і таке інше виділяється деяка, характерна тільки для нього, послідовність байтів. Ця послідовність називається сигнатурою даного вірусу. Пошук вірусів, у найпростішому випадку, зводиться до пошуку їх сигнатур. Після виявлення вірусу в тілі програми (або завантажувального сектора, який теж, містить програму початкового завантаження) поліфаг знешкоджує його. Для цього розробники антивірусних засобів ретельно вивчають роботу кожного конкретного вірусу: що він псує, як він псує, де він ховає те, що зіпсує та інше. Сканування є найбільш традиційним методом пошуку вірусів. Воно полягає в пошуку сигнатур, виділених з раніше виявлених вірусів. Вірусні бази сучасних сканерів містять більше 40 000 масок вірусів.

Недоліком простих сканерів є їх нездатність виявляти "поліморфні" віруси, що повністю міняють свій код. Сучасні поліфаги використовують інші методи пошуку таких вірусів. Для цього вони використовують більш складні алгоритми пошуку, що включають евристичний аналіз перевірки програм. Враховуючи, що постійно з'являються нові віруси, програми-детектори та програми-поліфаги швидко застарівають, і потрібно регулярне оновлення версій баз даних, що містять сигнатури нових вірусів. Як результат, сканери застарівають вже в момент виходу нової версії.

Евристичні аналізатори – перевіряють програми і виявляють дії, характерні для вірусів. Завдяки цьому евристичні аналізатори здатні знаходити "поліморфні" віруси також легко, як і звичайні віруси, які не використовують механізму маскування, крім того, вони можуть виявляти віруси, раніше невідомі авторам антивірусної програми.

Для виявлення зазначених вірусів використовуються спеціальні методи. До них можна віднести метод емуляції процесора. Метод полягає в імітації виконання процесором програми і підсовування вірусу фіктивних керуючих ресурсів. Обманутий таким чином вірус, що знаходиться під контролем антивірусної програми, розшифровує свій код. Після цього, сканер порівнює розшифрований код з кодами зі своєї бази даних сканування.

Для більш надійного захисту комп'ютерних систем від вірусних атак все більшого поширення набувають антивірусні комплекси.

Антивірусний комплекс – набір антивірусів, що використовують однакове антивірусне ядро, яке призначено для вирішення практичних проблем щодо забезпечення антивірусної безпеки комп'ютерних систем. В антивірусний комплекс також в обов'язковому порядку входять засоби відновлення антивірусних баз.

Будь-яка локальна мережа, як правило, містить комп'ютери двох типів: робочі станції, за якими безпосередньо працюють люди, і мережеві сервери, що використовуються для службових цілей. Відповідно до характеру виконуваних функцій сервери поділяються на:

мережеві, які забезпечують централізоване сховище інформації: файлові сервери, сервери додатків та інші;

поштові, на яких працює програма, що служить для передачі електронних повідомлень від одного комп'ютера до іншого;

шлюзи, що відповідають за передачу інформації з однієї мережі в іншу. Наприклад, шлюз необхідний для з'єднання локальної мережі з Інтернетом.

Відповідно, розрізняють чотири види антивірусних комплексів: для захисту робочих станцій, файлових серверів, поштових систем і шлюзів.

Робочі станції – це комп'ютери локальної мережі, за якими безпосередньо працюють користувачі. Головним завданням комплексу для захисту робочих станцій є забезпечення безпечної роботи на розглянутому комп'ютері – для цього необхідна перевірка в режимі реального часу, перевірка на вимогу і перевірка локальної електронної пошти.

Мережеві сервери – це комп'ютери, спеціально виділені для зберігання або обробки інформації. Вони зазвичай не використовуються для безпосередньої роботи за ними, і тому, на відміну від робочих станцій, перевірка електронної пошти на наявність вірусів тут не потрібна. Отже, антивірусний комплекс для файлових серверів повинен проводити перевірку в режимі реального часу і перевірку на вимогу.

Антивірусний комплекс для захисту поштових систем призначений для перевірки всіх електронних листів на наявність в них вірусів. Тобто перевіряти інші файли, розміщені на цьому комп'ютері, він не зобов'язаний (для цього існує комплекс захисту мережевих серверів). Тому до нього пред'являються вимоги щодо наявності програми для перевірки всієї поштової кореспонденції в режимі реального часу і додатково механізму перевірки на вимогу поштових баз даних.

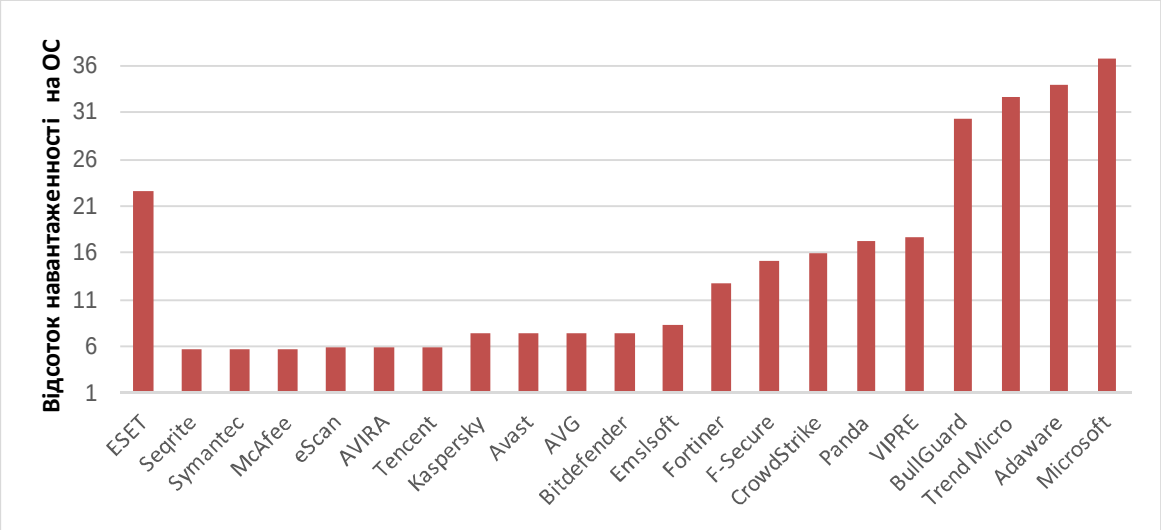
Аналогічно, згідно зі своїм призначенням, антивірусний комплекс для шлюзу здійснює перевірку даних, що проходять через шлюз.

Оскільки всі перераховані вище комплекси використовують сигнатурний аналіз, то в обов'язковому порядку в них повинен входити засіб для підтримки антивірусних баз в актуальному стані, тобто механізм їх оновлення. Часто виявляється корисним модуль для віддаленого централізованого управління, який дозволяє системному адміністраторові зі свого робочого місця налаштовувати параметри роботи антивірусу, запускати перевірку на вимогу і оновлення антивірусних баз.

Якщо розглядати технології захисту від шкідливих програм не окремо, а узагальнено, з точки зору представленої моделі, то складається наступна картина.

Технічний компонент технології відповідає в основному за такі її характеристики, як навантаження на систему (і як наслідок – її швидкодія), безпека та захищеність.

Навантаження на систему – це частка процесорного часу і оперативної пам'яті, безперервно або періодично задіяних у забезпеченні захисту і обмежує швидкодію системи. Емуляція виконується повільно, незалежно від реалізації: на кожну проемульовану інструкцію доводиться кілька інструкцій штучного середовища. Те ж можна сказати і про віртуалізацію. Моніторинг системних подій також безумовно рівномірно гальмує всю систему. На рис. 2 показаний графік впливу антивірусних засобів на операційну систему персонального комп'ютера за травень місяць 2017 року [6].



Під "безпекою" мається на увазі ступінь ризику, якому піддається операційна система і дані користувача в процесі ідентифікації потенційно шкідливого коду. Такий ризик існує завжди, коли шкідливий код виконується реально, в операційній системі. Для систем моніторингу подій таке реальне виконання коду архітектурно обумовлено, в той час як емуляція і файлове сканування можуть виявити шкідливий код ще до того, як він почав виконуватися.

Захищеність, цей параметр відображає уразливість технології, те, наскільки шкідливий код може ускладнити процес ідентифікації себе. Протистояти файловому детектуванню дуже легко: достатньо добре упакувати файл, зробити його поліморфним, або скористатися руткіт-технологією для приховування файлу. Протистояти емуляції трохи складніше, але також можливо для цього використовуються численні трюки, вбудовані в код шкідливої програми. Але сховатися від системного моніторингу програми вже складно – з тієї причини, що практично неможливо приховати поведінку.

В середньому, чим менш абстрактний захист, тим він безпечніше, але й тим простіше його обійти.

Аналітичний компонент технології відповідає за такі характеристики, як проактивність (і залежну від неї необхідну частоту оновлення антивірусу), відсоток помилкових спрацьовувань і навантаження на користувача.

Під проактивністю мається на увазі здатність технології виявляти нові шкідливі програми, які ще не потрапили до рук фахівців. У міру зростання складності аналітичної системи, зростає і її проактивність. З проактивністю безпосередньо пов'язана і така характеристика системи захисту, як необхідність постійного оновлення.

Наприклад, бази сигнатур потрібно постійно оновлювати, в той час як більш складні евристичні системи залишаються адекватними до поточної ситуації більш тривалий термін, а експертні аналітичні системи можуть успішно функціонувати без оновлень місяцями.

Відсоток помилкових спрацьовувань так само безпосередньо пов'язаний зі складністю технології аналізу. Якщо шкідливий код ідентифікується жорстко заданою сигнатурою або послідовністю дій, за умови достатньої довжини сигнатури.

Під навантаженням на користувача мається на увазі ступінь його участі у формуванні політики захисту – правил, винятків, білих і чорних списків – і участі в процесі винесення вердикту – підтвердження або спростування "підозр" аналітичної системи.

Чим складніша аналітична система, тим вона могутніша, але і тим вище відсоток помилкових спрацювань.

Висновки й перспективи подальших досліджень

На даний момент більшість рішень в області комп'ютерної безпеки реалізуються, як комплекс декількох технологій. У класичних антивірусах сигнатурні детектування зазвичай використовується в парі з тією чи іншою реалізацією моніторингу системних подій, емулятора, пісочниці.

Перш за все, слід пам'ятати, що не існує ні універсального, ні "найкращого" рішення. У кожної технології є свої плюси і мінуси. Наприклад, моніторинг подій в системі постійно займає процесорний час, але його найважче обманути; процесу емуляції можна перешкодити використанням в коді певних команд, але при її використанні виявлення шкідливого коду виконується в попереджуючому режимі, система залишається захищеною. Вибір технології – це вибір золотої середини з урахуванням конкретних потреб і обставин.

Існує безліч методик виявлення невідомого шкідливого програмного засобу. Кожна з них має свої переваги, недоліки та особливості використання. Але на даний момент не існує методики, яка б повністю вирішувала завдання виявлення невідомого шкідливого програмного засобу з прийнятною ефективністю для будь-яких видів шкідливих програмних засобів і за будь-яких вимог до системи виявлення шкідливих програмних засобів. Теоретично об'єднання декількох методик може вирішити цю проблему.

Для проведення ефективного дослідження комп'ютера, пошуку і знищення шкідливих програм потрібно комбінувати всі методи, способи і засоби, які висвітлені в цій статті.

Література

1. Безруков Н. Компьютерная вирусология. /Безруков Н.// - К.: УРЕ, 1991. с. 15. **2. Гульев И.** Компьютерные Вирусы. Взгляд Изнутри. /Гульев И.// - М.: ДМК 1998. с. 58-62. **3. Козлов Д.А.** Энциклопедия компьютерных вирусов. /Козлов Д.А., Парандовский А.А., Парандовский А.К.// Издательство: СОЛОН - Р, 2010. с. 343. **4. Собейкис В.Г.** Азбука хакера 3. /Собейкис В.Г.// - С.: Компьютерная вирусология, 2014. с. 26-28. **5. Шаньгин В.** Защита информации в компьютерных системах и сетях. /Шаньгин В.// - ДМК Пресс 2013. с. 65. **6. AV-Comparatives** – Незалежні тести антивірусного програмного забезпечення. / [Електронний ресурс] // - Режим доступу: www.av-comparatives.org – Назва з екрану.

МЕТОДЫ И СРЕДСТВА ПРОТЕВОДЕЙСТВИЯ ВРЕДОНОСНОМУ ПРОГРАМНОМУ ОБЕСПЕЧЕНИЮ

Вадим Иванович Пеньков
Роман Михайлович Штонда
Александр Николаевич Гук
Ирина Робертовна Мальцева
Юлия Александровна Черныш

Военный институт телекоммуникаций и информатизации, Киев, Украина

Информационные технологии определяют процессы передачи, хранения и обработки информации, а также её использование в определенных целях. Эти процессы должны быть быстрыми, менее затратными, максимально полезными, удобными и автоматизированными. По этой причине основной тенденцией развития информационных технологий является их представление в цифровом виде, переход к цифровым информационно-телекоммуникационных базам, основанным на цифровом взаимодействия компьютеров, разработанных с самыми разнообразными функциональными алгоритмами. Внедрение персональных компьютеров в информационную сферу и применение телекоммуникационных средств связи определили новый этап развития информационных технологий.

Развитие Интернета изменило отношение к проблемам безопасности, подняв вопрос о защищенности локальных и глобальных компьютерных сетей. Еще недавно эти проблемы не были столь актуальными. Разработчики первых компьютерных сетей в первую очередь стремились увеличить скорость и надежность передачи данных, порой достигая желаемого результата в ущерб безопасности.

Увеличение скорости передачи информации, объемов и значимости обрабатываемых в вычислительных сетях данных открывает перед киберпреступниками все более широкие возможности. Распространение по всему миру вредоносного программного обеспечения занимает считанные дни или даже часы. Сотни мегабайт оперативной памяти позволяют выполнять практически любые действия незаметно для пользователя. Спектр возможных целей, таких как пароли, карточные счета, ресурсы удаленных компьютеров представляет огромное поле для их деятельности.

Ключевые слова: *вредоносное программное обеспечение, антивирусные программы, компьютерный вирус, компьютерная система, компьютерная сеть.*

METHODS AND MEANS OF PROTECTION FROM MALICIOUS SOFTWARE

Vadym I. Penkov, Roman M. Shtonda, Oleksandr M.Guk,
Iryna R. Maltseva, Yuliia A. Chernysh

Military Institute of Telecommunications and Information, Kyiv, Ukraine

Information technologies define the processes of transmission, storage and processing of information, as well as its use for certain purposes. These processes should be fast, less expensive, as useful as possible, convenient and automated. For this reason, the main trend in the development of information technologies is their presentation in digital form, the transition to digital information and telecommunications bases based on the digital interaction of computers developed with a wide variety of functional algorithms. The implementation of personal computers into the information sphere and the use of telecommunications means of communication have determined a new stage in the development of information technologies.

The development of the Internet has changed attitudes to security issues, raising the issue of the security of local and global computer networks. Until recently, these problems were not so relevant. Developers of the first computer networks primarily sought to increase the speed and reliability of data transmission, sometimes achieving the desired result to the detriment of security.

The increase in the speed of information transfer, the volumes and significance of data processed in computer networks opens up wider opportunities for cybercriminals. Distribution around the world of malicious software takes a few days or even hours. Hundreds of megabytes of random access memory allow you to perform virtually any actions imperceptibly for the user. A range of possible goals, such as passwords, card accounts, remote computer resources, is a huge field for their activities.

Keywords: *malicious software, antivirus software, computer virus, computer system, computer network.*

References

1. Bezrukov N. (1991) Computer virology. [*Komp'yuternaya virusologiya.*]- K.: URE, p. 15. **2. Gul'yev I.** Computer viruses. View from the inside [*Komp'yuternyye Virusy. Vzglyad Iznutri*] - M.: DMK 1998. pp. 58-62. **3. Kozlov DA,** Parandovsky AA, Parandovsky A.K. (2010) Encyclopedia of computer viruses. [*Entsiklopediya kompyuternyih virusov*] Publisher: SOLON-R p. 343. **4. Sobeykis V.G.** (2014) The ABC of the hacker 3. [*Azbuka hakera 3*] S.: Computer virology pp. 26-28. **5. Shanguin V.** (2013) Protection of information in computer systems and networks. [*Zaschita informatsii v kompyuternyih sistemah i setyah.*] DMK Press p. 65. **6. AV-Comparatives** (2017) Independent Tests of Anti-Virus Software [*Nezalezhni testy antyvirusnoho prohramnoho zabezpechennia*], www.av-comparatives.org.