ПЛАН

Вступ

Як відомо, в англомовній літературі для позначення продукції, пов'язаної з інформатикою, широко використовуються терміни "Hard Ware" (жорсткий продукт, технічні засоби, комп'ютери) та "Soft Ware" (м'який продукт, програми, програмне забезпечення). З масовим поширенням персональних комп'ютерів (ПК) з'явився новий термін "Bad Ware" (поганий продукт). До останнього відносять в першу чергу комп'ютерні віруси, троянських коней та черв'яків.

Далі основну увагу присвятимо комп'ютерним вірусам. Ми розглянемо, що таке комп'ютерні віруси, як вони себе проявляють і якої шкоди можуть заподіяти, наведемо декілька їх класичних і сучасних прикладів і, нарешті, обговоримо засоби боротьби з ними. Для поглибленого вивчення цих питань можна використати монографію відомого київського вірусолога М.Безрукова "Компьютерные вирусы" [1].

Відносно двох останніх видів "поганого продукту" зауважимо таке.

Комп'ютерні троянські коні, як і їх міфічні попередники, маскують свої дії під виглядом благопристойної, безневинної продукції, завдаючи болісні, руйнівні удари по вашій інформації. В той же час функцій розмноження, зараження інших програм, на відміну від вірусів, троянські коні не мають. Їм часто присвоюються точні (або дуже схожі) імена широко відомих комп'ютерних програм. Свого часу троянські коні набули такого поширення, що солідні комп'ютерні журнали щомісяця друкували їх довгі списки.

Комп'ютерні черв'яки являють собою програми, які призначені для проникнення через інформаційні мережі до даних, що зберігаються в інших фірмах, установах тощо. Зрозуміло, що робиться це з корисливих міркувань.

Відзначимо також, що створення та розповсюдження вірусів, троянських коней та черв'яків, незважаючи на мотиви цього, є, безумовно, шкідливими для суспільства діями, що завдають значних матеріальних збитків. Ось чому у деяких країнах ці дії розглядаються як карний злочин і переслідуються законом. На жаль авторів "поганої продукції" знайти дуже нелегко!

1. Поняття про комп’ютерний вірус

Із загальної точки зору комп'ютерні віруси являють собою програми, які мають здатність до прихованого розмноження у середовищі операційної системи за допомогою включення у код, що виконується, (програми, компоненти операційної системи, пакетні файли, текст, що компілюється, тощо) своєї, можливо модифікованої копії, яка зберігає здатність до подальшого розмноження. Крім функції розмноження (зараження інших

файлів) комп'ютерні віруси виконують, як правило, ті чи інші деструктивні дії, про які мова бути йти далі.
Цей варіант належить М.Безрукову і базується на означенні, даному у 1989р. Ф.Коуеном (F.Cohen) — піонером першого серйозного дослідження комп'ютерних вірусів.
За способом зараження більшість комп'ютерних вірусів можна підрозділити на два класи: файлові та бутові віруси. Розглянемо коротко механізми їх дії.
Найпоширенішим засобом зараження файлу вірусом є дописування його тіла у кінець файлу (див. рис. 1). При цьому, щоб при запуску зараженого файлу одразу одержати управління, вірус замість початку файлу, який приховує у своєму тілі, ставить команду переходу на себе. Після того, як вірус відпрацював, він передає управління файлу-жертві. В деяких випадках, якщо в силу тих чи інших причин початок файлу, що інфікується, не зберігається, або є ще якісь "помилки" у вірусі, файл буде зіпсований і його подальше лікування буде неможливим.
Останнім часом поширились віруси, що перезаписують початок файлу-жертви (File Overwriters), не змінюючи його довжину. Зрозуміло, що інфікована таким чином програма замість свого дійсного початку містить вірус і буде безповоротно зіпсована, залишаючись в змозі лише заражати інші програми. Як правило, вказані віруси під час своєї дії інфікують якомога більше файлів і, в залежності від різних умов, виконують ті чи інші додаткові руйнівні дії. Прикладами цих вірусів є: ABRAXAS-3, BANANA, BURGER, BLOODLUST, BK MONDAY, COSSIGA, CLINT, DRUID та багато інших.
Зауважимо, що віруси можуть записувати своє тіло також у кінець або середину файлу-жертви. Останнім часом з'явились віруси, які впроваджують себе до файлу, що заражається окремими "плямами". При запису у середину файлу вірус інколи знаходить "порожні" місця і приміщує туди своє тіло, не змінюючи довжину жертви. У більшості випадків довжина інфікованого файлу збільшується на деяку величину, що, як правило, є постійною для вірусу, який заразив його. Ця величина зветься довжиною вірусу і вимірюється звичайно у байтах. У більшості випадків віруси пишуться на мові Асемблера, інколи на мовах високого рівня (Pascal, C тощо). У першому випадку довжина вірусів порівняно невелика (SillyCR.76 — мабуть, світовий рекордсмен малих резидентних вірусів, що зберігає працездатність інфікованої програми, має довжину у 76 байт), у другому — може бути у декілька десятків Кбайт (MiniMax — 31125 байт). Цікаво, що існують віруси (DICHOTOMY), які при зараженні записують частини свого тіла у два різних файли (296 + 567 байт).

Важливою характеристикою вірусів є здатність багатьох з них залишатись у пам'яті комп'ютера після запуску інфікованого файлу. Такі віруси називають резидентними. Зрозуміло, що резидентні віруси уражають файли набагато частіше ніж нерезидентні. Бутові віруси заражають Boot-сектор вінчестера або дискет. Вірус записує початок свого тіла до Boot-сектора, а решту у вільні (інколи зайняті) кластери, помічаючи їх як погані. Туди ж вірус приміщує також і справжній запис Boot-сектора, щоб потім передати йому управління. За своєю природою бутові віруси завжди резидентні.

Останнім часом з'явились окремі віруси, які заражають і Boot-сектори (або Master Boot записи) і файли. Такі віруси звуться файлово-бутовими (Multi-Partite Viruses). Прикладом таких, поки що дуже рідких вірусів, є вірус One_Half, що розглядається далі.
Крім того є віруси, механізм зараження яких суттєво відрізняється від розглянутих вище

механізмів. Першим таким вірусом був вірус DIR. Цей вірус не заражував виконувані файли, а лише змінював у каталогах посилання на початок файлу-жертви, так щоб воно тепер вказувало на тіло вірусу, який містився в єдиному екземплярі на всьому диску. Таким чином при запусканні будь-якої зараженої програми вірус одержував управління першим, а після відпрацювання передавав управління запущеній програмі.

Сучасні віруси застосовують найрізноманітніші засоби, з метою утруднити роботу по їх виявленню, розшифруванню та знешкодженню.
В поліморфні віруси (Self-Encrypting Polymorphic Viruses) встроюються так звані поліморфні генератори вірусних шифрувальників та розшифрувальників (MtE — MuTation Engine — механізми утворення поліморфних копій), які змінюють їх коди з часом.
Значна частина сучасних вірусів використовує так звану Stelh-технологію (за аналогією із назвою відомого літака). Ці віруси-невидимки самоліквідуються при спробі дослідження їх за допомогою відповідних засобів (відлагоджувачі та трасувальники), видають інформацію, начебто уражений комп'ютер не має інфекції і т.п. Так, вже один із перших вірусів BRAIN при спробі проглядання зараженого Boot-сектора виводив не своє тіло, що знаходилось там, а справжній не інфікований запис. Вірус DARK AVENGER "підправляв" дію команди DIR операційної системи так, щоб довжина зараженого ним файлу виводилась без урахування довжини вірусу, тобто справлялось враження, що файл не інфікований.
Віруси-супутники (Companion Viruses) замість зараження існуючого EXE-файлу, утворюють новий файл, який має теж саме ім'я, але інше розширення (COM). Сам вірус буде знаходитись у знов утвореному файлі. Наприклад, для файлу EDIT.EXE буде утворений файл EDIT.COM і сам вірус буде знаходитись в останньому файлі. При спробі запуску EXE-програми з командного рядка, замість потрібної програми буде запущена знов утворена, з вірусом. Після її відпрацювання буде запущена потрібна програма (EXE).
На ранніх етапах розвитку віруси заражали лише виконувані файли типу COM та EXE. Зараз спектр файлів, що можуть зазнавати атаки з боку вірусів значно розширився. Відмітимо, що існують віруси, які можуть заражати файли в архівах (типу ARJ, ZIP тощо), файли-документи (типу DOC), що утворені відомим текстовим процесором WinWord (6 версія та вище) фірми MicroSoft.
Деякі віруси залишаються у пам'яті ПК після теплого перезавантаження (Ctrl+Alt+Del). Більше того, при спробі завантажити чисту операційну систему з пристрою A: після холодного запуску, тобто після натискання кнопки Reset або вимкнення/увімкнення комп'ютера, ви можете несподівано виявити, що у його пам'яті вже знаходиться вірус. Саме такі можливості мають віруси EXEBUG та MAMMOTH, які відключають у CMOS'і наявність дисководу A:, що призводить до завантаження зараженої системи з диску C:. При цьому вірус імітує, начебто завантаження відбувається саме з гнучкого диска. Якщо ж на зараженій машині ви звернетесь до дисководу A:, то він буде тимчасово включений. У порівнянні з такими монстрами змінювання системного часу в CMOS'і деякими вірусами виглядає як безневинна забава!
І останній приклад "швидкого реагування" вірусів на нові досягнення комп'ютерної техніки. Тільки-но з'явився так званий Flash-BIOS, як вірус VLAD став записувати свій код до нього.

2. Приклади комп'ютерних вірусів

Як ми вже казали, комп'ютерні віруси підрозділяються на два основних класи: файлові та бутові. Розглянемо деякі з них більш докладно.

Файлові віруси

Вірус VIENNA (Відень)

Інші назви вірусу: 648, Restart (перезавантаження), Time Bomb (часова бомба) та ін.

Один із перших найбільш примітивних вірусів. Знайдений спочатку у Відні, потім заполонив увесь світ. При завантаженні у пам'ять комп'ютера проглядає всі COM-програми у поточному каталозі та у доступних через PATH (шляхи пошуку, що звичайно встановлені в AUTOEXEC.BAT). Первісний варіант цього вірусу збільшував довжину жертви на 648 байт. Першу знайдену ще не заражену програму або заражає, або, з ймовірністю 1/8 (в залежності від системного часу), псує таким чином, що вона при запуску призводить до перезавантаження системи. В останньому випадку в початок жертви записується код EAF0FF00F0, який на машинній мові означає теплий рестарт (еквівалентне до дії клавіш Ctrl+Alt+Del). Якщо зіпсована таким чином програма викликається з AUTOEXEC.BAT, процедура початкового завантаження операційної системи зациклюється. Як ознаку зараження, вірус ставить у часі створення жертви неіснуюче число секунд (62). Надалі з'явилось багато різновидів вірусу VIENNA (більше 20), що відрізняються від нього довжинами та шкідливими діями.

Вірус CASCADE (Каскад, водоспад)

Інші назви вірусу: LetterFall (буквопад), Letter та ін.

Існує два варіанти вірусу за довжиною (1701 або 1704 байт). Заражає тільки COM-програми, резидентний. Спричиняє обсипання символів на екрані, що супроводжується характерним шелестінням. При цьому блокується можливість роботи з клавіатурою. Зберігає працездатність тільки на машинах типу PC XT/AT.

Вірус BLACK FRIDAY (Чорна п'ятниця)

Інші назви вірусу: Israeli Virus (ізраїльський вірус), Ierusalem (Єрусалим), Black Hole (чорна дірка) та ін.

Вірус одержав вказані назви, оскільки вперше був виявлений в ізраїльському університеті та із-за своїх характерних дій. Він заражає EXE- та COM-файли, збільшуючи їх розміри на 1813 байт, і залишається резидентним у пам'яті ПК. При цьому зараження може відбуватися неодноразово, що приводить до неймовірного розростання заражених файлів. Інфікований даним вірусом ПК сповільнює свою роботу в декілька тисяч разів. При виведенні інформації на дисплей у нижньому лівому куті екрана з'являється чорний прямокутник (дірка). Нарешті, якщо час роботи приходиться на п'ятницю 13-го числа, то заражені файли знищуються.

Характерною ознакою вірусу є наявність в його тілі сполучень MsDos а також COMMAND.COM.

Вірус DARK AVENGER (Чорний месник)

Інші назви вірусу: Eddie, Sofia.

Вірус одержав свої назви по текстовому рядку "Eddie lives ... somewhere in time. This program was written in the sity of Sofia (C) 1988-89 Dark avenger", що міститься у його тілі. Вірус заражає EXE- та COM-файли, є резидентним, його довжина в байтах — 1800. Вірус дуже небезпечний, оскільки на інфікованому комп'ютері файли заражаються не тільки при виконанні, але і під час їх проглядання та копіювання. Він також знищує COM-файли, довжина яких лежить у межах від 64K–1800байт до 64K. Періодично

знищує інформацію в одному із секторів вінчестера.

Бутові віруси

Вірус PING PONG (назва не потребує перекладу)

Інші назви вірусу: Italian Bouncing (італійський стрибунець), Ball (м'ячик).

Вірус заражає Boot-сектор дискет і записує своє тіло у вільні (інколи і у зайняті) кластери, помічаючи їх як погані (Bad). Як і всі бутові віруси є резидентним. На ПК, зараженому даним вірусом, час від часу з'являється ромбик (ASCII-код—4), який, переміщуючись по екрану, відбивається від його границь та рамок, утворених символами псевдографіки.

Вірус STONED (Закам'янілий)

Інша назва вірусу: Marijuana (Маріхуана).

Зовнішнє проявлення — з ймовірністю 1/8 під час завантаження системи на екран видається текст "Your PC is now Stoned", після чого робота нормально продовжується. Цей вірус записується в абсолютний початковий сектор диска, який на вінчестерах містить PARTITIONTABLE. Інколи (наприклад, коли жорсткий диск розбитий на розділи за допомогою відомої системи ADM) це приводить до сумних наслідків, а саме, до втрати доступу до інформації, розташованої на диску. Для візуального розпізнання вірусу на диску може служити палкий заклик: "LEGALISE MARIJUANA!".

Зауважимо, що зараз існує близько 90 штамів (різновидів) вірусу Stoned, і він досі залишається дуже поширеним.

Вірус BRAIN (Мозок)

Один із найбільш знаменитих вірусів. Він вважається першим, що одержав широке розповсюдження (розроблений у січні 1986 року). Заражає тільки стандартно відформатовані дискети ємністю 360K. На заражених дискетах з'являється мітка "(c)Brain". Займає на диску три підряд розташованих кластери, помічаючи їх як погані.

Нарешті, для любителів футболу наведемо останній приклад продукту, судячи по всьому, вітчизняного виробництва.

Вірус DINAMO (назва не потребує перекладу)

Це бутовий вірус, який при деяких обставинах видає на екран вічну мрію київських уболівальників: "Dinamo (Kiev) – champion!!!".

3. Антивірусні програми

Антивірусні програми за своїм призначенням поділяються на детектори, фаги, ревізори, фільтри та вакцини. Розглянемо їх характеристики більш докладно.

Детектори служать тільки для виявлення вірусів у комп'ютері. Фаги лікують його від вірусної інфекції. Дуже часто функції детектора та фага суміщені в одній програмі, а вибір режиму роботи здійснюється завданням відповідних параметрів (опцій, ключів). На початку вірусної ери кожний новий вірус визначався та лікувався окремою програмою. При цьому для деяких з вірусів (наприклад, VIENNA) цих програм було не менше десятка. Згодом окремі програми почали виявляти та лікувати декілька типів вірусів, тому їх стали звати полідетекторами та поліфагами відповідно. Сучасні антивірусні програми знаходять і знешкоджують багато тисяч різновидів вірусів і заради простоти їх звуть коротко детекторами та фагами. Серед детекторів та фагів найбільш відомими та популярними є програми Aidstest, DrWeb (фірма ДиалогНаука, Росія), Scan, Clean (фірма McAfee Associates, США), Norton AntiVirus (фірма Symantec Corporation, США). Ці програми періодично (в середньому двічі на місяць) поновлюються, даючи користувачеві

змогу боротися з новими вірусами. Показником важливості антивірусних засобів стало включення до складу операційної системи MS-DOS утиліти MSAV (MicroSoft AntiVirus). Щоправда, цей продукт був розроблений фірмою Central Point Soft Ware (автором славнозвісних PCTools та PCShell) і звався CPAV, а згодом був куплений фірмою MicroSoft. Утиліта MSAV є одночасно детектором, фагом, ревізором та вакциною.
Під час запуску фагів у пам'яті комп'ютера не повинно бути резидентних антивірусних програм, які блокують запис на диск (фільтрів).
Ще одним типом антивірусних програм є ревізори. Ці програми можуть виявляти факт зараженості комп'ютера новими вірусами, слідкуючи за всіма змінами системних областей та файлової структури на вашому ПК. При першому запуску ревізор утворює таблиці, куди заносить інформацію про вільну пам'ять, Partition Table, Boot, директорії, файли, що містяться у них, погані кластери тощо. При повторному запуску ревізор сканує пам'ять та диски і видає повідомлення про всі зміни, що відбулися у них з часу останнього сеансу ревізії. Нескладний аналіз цих змін дозволяє надійно визначити факт зараження комп'ютера вірусами. Серед ревізорів, мабуть, найбільш популярною є програма ADinf (фірма ДиалогНаука, Росія). Вже згадувана програма MSAV також може виконувати функції ревізора.
Свого часу, коли не було надійних засобів боротьби з вірусами, широкого поширення набули так звані фільтри. Ці антивірусні програми блокують операцію записування на диск і виконують її тільки при вашому дозволі. При цьому легко визначити, чи то ви санкціювали команду на запис, чи то вірус намагається щось заразити. До числа широко відомих свого часу фільтрів можна віднести програми VirBlk, FluShot, Anti4us. До речі, остання програма — німецького виробництва і при читанні її назви ми одержимо щось на зразок "антивірус". Зараз фільтри майже не використовують, оскільки вони, по-перше, дуже незручні, бо відволікають час на зайвий діалог, по-друге, деякі віруси можуть обманювати їх. Відмітимо утиліту П.Нортона DISCMON, яка у режимі Protect здійснює саме функцію фільтра.
Нарешті до антивірусних програм відносяться вакцини. Зауважимо відразу, що їх поширення було дуже обмеженим раніше, а зараз вони практично зовсім не використовуються. Справа у тому, що вакцини призначені для боротьби з дуже обмеженими класами вірусів і для кожного їх типу потребують досить складної розробки відповідних програм. Пояснимо на прикладах суть дії вакцин. Як ми вже казали раніше, вірус VIENNA проставляє у зараженому файлі неіснуючий час утворення (62 секунди). Це ж саме робить і вакцина проти вказаного вірусу. Аналогічно, вакцина проти вірусу BLACK FRIDAY використовує той факт, що цей вірус прикметою зараженості використовує сполучення MsDos, що записується у кінець файлу-жертви.
Розглянемо тепер деякі із згаданих вище антивірусних програм.
Антивірусна програма Aidstest Д.Лозинського
Ця програма є детектором та фагом одночасно і, отже, призначена для виявлення і лікування файлів та Boot-секторів, які заражені відомими типами вірусів. В процесі роботи програмні файли, які виправити неможливо, витираються.
Програма викликається таким командним рядком (вказані тільки основні параметри):
Aidstest path[/f][/g][/s][/p[ім'я файлу]][/q][/e]
Параметри програми:
path задає підмножину файлів для перевірки на зараженість. Кодується практично за тими ж правилами, що і в команді DIR операційної системи. Замість цього параметра

можна поставити символ "*", що задає роботу з усіма логічними розділами жорстких дисків, або символи "**", які задають роботу з усіма дисками, починаючи з "C:" і включаючи ті, що працюють у мережі, CD та subst-диски. Для перевірки поточного каталогу задається просто символ ".";
/f лікувати заражені програми та витирати безнадійно зіпсовані;
/g глобальна перевірка всіх файлів (не тільки COM, EXE та SYS). З цим параметром програму рекомендується запускати лише тоді, коли відомо про наявність у комп'ютері вірусів;
/s використовується у випадку, коли вірус, об'явлений видаленим, продовжує з'являтися знову;
/p[ім'я файлу] виводить протокол роботи. Якщо ім'я файлу не задане, виведення відбувається на принтер без нагадування;
/q виводить підказку про дозвіл на витирання безнадійно зіпсованих файлів.
Якщо ви запустили програму без параметрів або помилилися при їх завданні, на екран видається короткий опис параметрів програми.
Приклади використання програми Aidstest.
Aidstest * перевірка всіх EXE-, COM- і SYS-файлів на всіх дисках, починаючи з "C:".
Aidstest a: перевірка всіх EXE-, COM- і SYS-файлів на дискеті в пристрої "A:".
Aidstest d:/g/f лікування всіх доступних файлів на диску "D:".
Під час роботи програма Aidstest виводить повідомлення, зміст яких достатньо простий та зрозумілий.
Антивірусна програма DrWeb І.Данилова
Ця програма є детектором та фагом одночасно і призначена для виявлення і лікування програм, які заражені відомими типами вірусів. Крім того програма містить евристичний аналізатор, який, базуючись на загальних відомостях про характеристики та властивості вірусів, дозволяє інколи знаходити нові, невідомі їх екземпляри. Щоправда, це дещо уповільнює її роботу. Взагалі, серед тестованих журналом "Virus Bulletin" 25 відомих антивірусних програм DrWeb зайняв останнє місце за швидкодією. Програма DrWeb працює у зручному діалоговому режимі і добре документована.
Антивірусні програми Scan та Clean J.McAfee
Програма Scan є детектором, а програма Clean — фагом. За кількістю вірусів, які можуть виявляти та лікувати ці програми, вони посідають, мабуть, перше місце. Але краще все-таки користуватися двома попередніми програмами, оскільки зараз, як ми вже казали, центр виробництва вірусів перемістився на територію колишнього СРСР, а програми Aidstest та DrWeb швидше "реагують" на них.
Під час своєї роботи програма Scan у разі виявлення зараженості комп'ютера повідомляє ім'я відповідного вірусу. Для лікування треба задати це ім'я для програми Clean як параметр.
До складу комплексу програм J.McAfee входить також ревізор Validate.
Антивірусна програма Norton AntiVirus
Остання версія цього продукту — перша, яка почала працювати у середовищі операційної системи Windows-95, використовуючи всі її особливості та можливості. Система Norton AntiVirus пропонує користувачеві чудовий діалоговий режим боротьби з вірусами, в якому передбачений цілий комплекс засобів, зокрема, створення рятувальної (Rescue) дискети. Ця система є одночасно детектором, фагом та ревізором.
Антивірусна програма ADinf Д.Мостового

Ця програма є одним з найпоширеніших ревізорів, дуже швидко проглядає весь диск і повідомляє у зручній діалоговій формі про всі підозрілі зміни на ньому. Програма має простий, інтуїтивно зрозумілий інтерфейс та добре документована. Додатково з ADinf може працювати спеціальний модуль, що лікує, ADinf Cure Module, який дозволяє у багатьох випадках зараження новими вірусами успішно відбудовувати уражені файли.
Антивірусна програма AVP Є.Касперського
Ця програма менш популярна, ніж Aidstest та DrWeb, але містить у своєму складі чудову демонстрацію роботи багатьох вірусів.

Список використаної літератури

1. Безруков Н.Н. Компьютерная вирусология: Справ. руководство. — К.: УРЕ, 1991.— 416 с.
2. Касперский Е.В. Компьютерные вирусы в MS DOS. — М.: 1992.
3. Хижняк П.Л. Пишем вирус... и антивирус. — М.: ИНТО, 1991. — 90 с.