Міністерство освіти і науки, молоді та спорту України

Тернопільський національний педагогічний університет

імені Володимира Гнатюка

Кафедра інформатики

та методики її викладання

Реферат на тему:

«Виявлення і ознаки комп’ютерних вірусів»

Виконала

Студентка 1-го курсу

Попович Анастасія

Науковий керівник:

Галан В. І.

Тернопіль – 2014

[Анотація 2](#_Toc379476859)

[Вступ 3](#_Toc379476860)

[Частина 1 4](#_Toc379476861)

[Як дізнатися, чи інфіковано комп’ютер вірусом? 4](#_Toc379476862)

[Частина 2 5](#_Toc379476863)

[Різновиди вірусів: 5](#_Toc379476864)

[Частина 3 7](#_Toc379476865)

[Схема дії вірусів: 7](#_Toc379476866)

[Висновок 10](#_Toc379476867)

[Практична частина 11](#_Toc379476868)

[Посилання: 12](#_Toc379476869)

Анотація

У цьому рефераті я вияснила питання про такі поняття, як вірус, ризик зараження комп’ютерним вірусом, основні види вірусів, ознаки зараження комп’ютерним вірусом. Також я детально розглянула принцип дії популярних і небезпечних вірусів, а саме: вірус CASCADE, вірус DARKAVENGER, вірус BLACKFRIDAY, вірус PING PONG, вірус STONED, вірус BRAIN, вірус DINAMO, Троянський кінь. В практичній частині я описала як ми діяли при проблемі зараження комп’ютером вірусами. Також у цій частині можна дізнатися з якими проблемами можна стикнутись при видаленні вірусів.

Вступ

Ми живемо у час коли у кожного є свій персональний комп’ютер. Комп’ютерна індустрія розвивається з шаленою швидкістю. Але разом із тим зростає загроза зараження комп’ютера різними вірусами. Ось коротка характеристика різних видів і груп вірусів:

1) Завантажувальні віруси;

2) Файлові віруси;

3) Завантажувально-файлові віруси;

4) STEALTH-віруси;

5) Ретровірусами;

6) Multipartition – віруси.

Вони заражують ПК знищуючи інформацію, змінюючи параметри Windows, і заважаючи нормальні роботі операційні системі заторможуючи цим роботу ЦП і ОЗУ. Для захисту свого ПК були розроблені антивірусні програми, які появилися наприкінці 80-х років минулого століття, і які теж поділяються на типи за призначенням:

1) Детектори;

2) Фаги;

3) Ревізори;

4) Фільтри;

5) Вакцини;

Спочатку вони були дуже примітивними, адже до певного віруса треба було мати певний антивірус. В 1992 році комп’ютерна індустрія зробила великий скачок вперед. Російський програміст Ігор Данілов та його компанія “Діалог-Наука” розробили та випустили антивірусну програму Dr.WEB, яка поразила весь світ тим що, виявила 100% вірусів різних типів. За це компанія отримала нагороду від VisusBulettin. Так і до сьогоднішніх днів Dr.WEB являється одною з самих популярних антивірусних програм.

Частина 1

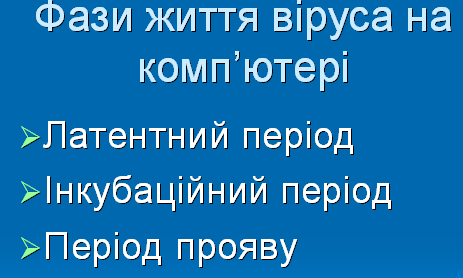
Як дізнатися, чи інфіковано комп’ютер вірусом?

**Комп’ютер працює надто повільно.** Поширений наслідок діяльності вірусу – значне сповільнення швидкодії комп’ютера. Однак можуть бути й інші причини повільної роботи, наприклад жорсткий диск, який необхідно дефрагментувати, малий обсяг оперативної пам’яті (ОЗП) комп’ютера або наявність шпигунської програми чи програмного забезпечення з рекламою.

**Відображення неочікуваних повідомлень або автоматичний запуск програм.** Деякі віруси можуть пошкодити операційну систему Windows або певні програми. Результатом цього пошкодження можуть бути повідомлення, що з’являються несподівано, автоматичний запуск або закриття програм чи раптове завершення роботи Windows.

**Модем або жорсткий диск перевантажено.** Вірус електронної пошти надсилає багато власних копій в електронних повідомленнях. Якщо постійно світиться індикатор роботи на високошвидкісному або зовнішньому модемі чи чути інший звук постійної роботи жорсткого диска, можливо, це ознаки діяльності вірусу. Це не завжди свідчить про наявність комп’ютерного вірусу, але в поєднанні з іншими проблемами може вказувати на інфікування ПК.

Щоб виявити віруси, виконайте перевірку комп’ютера будь-якою антивірусною програмою. Нові віруси з’являються майже щодня, тому важливо постійно оновлювати антивірусну програму.



1. Ознаки зараження вірусом:

* Зменшення вільної пам'яті;
* Уповільнення роботи комп'ютера;
* Затримки при виконанні програм;
* Незрозумілі зміни в файлах;
* Зміна дати модифікації файлів без причини;
* Незрозумілі помилки Write-protection;
* Помилки при інсталяції і запуску Windows;
* Відключення 32-розрядного допуску до диску;
* Неспроможність зберігати документи Word в інші каталоги, крім Template;
* Погана робота дисків;
* Файли невідомого походження.

Ранні ознаки зараження дуже тяжко виявити, але коли вірус переходить в активну фазу, тоді легко помітити такі зміни:

* Зникнення файлів;
* Форматування HDD;
* Неспроможність завантажити комп'ютер;
* Неспроможність завантажити файли;
* Незрозумілі системні повідомлення, звукові ефекти і т. д.

Здебільшого, все це в минулому. Зараз основні ознаки — самовільне відкривання браузером деяких сайтів (рекламного характеру), підозріло підвищений інтернет-трафік та повідомлення від друзів, що ваші листи електронної пошти до них містили вірус.

На додаток до цього віруси можуть без відома користувача виконувати інші довільні дії. З цієї причини віруси відносять до шкідливих програм.

Відомі сотні тисяч комп'ютерних вірусів, які поширюються через Інтернет по всьому світу.

Комп'ютерний вірус був названий за аналогією з біологічними вірусами за подібний механізм розповсюдження. По всій видимості, вперше слово «вірус» по відношенню до програми було вжито Грегорі Бенфордом (Gregory Benford) у фантастичному оповіданні «Людина у шрамах», опублікованому в журналі Venture в травні 1970 року.

Частина 2

Різновиди вірусів:

**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 BLACKFRIDAY** (Чорна п'ятниця)

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

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 DARKAVENGER** (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.

**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). Які 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 (Марихуана). 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 360К. 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!!!".

**Троянський кінь**

Це програма, що надає стороннім доступу до комп'ютера з метою будь-яких дій дома призначення без попередження самого власника комп'ютера або висилає за певним адресою зібрану інформацію. Частина троянських програм обмежується тим, що відправляє ваші паролі поштою своєму творцю чи людині, який конфігурував цю програму (е-mailtrojan). Проте задля користувачів Internet найнебезпечніші програми, які дозволяють одержати віддалений доступом до їх машині із боку (>BackDoor). Найчастіше трояни потрапляють на комп'ютер разом із корисними програмами чи популярними утилітами, маскуючись під них.



Частина 3

Схема дії вірусів:

Схема дії файлового вірусу

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.

Схема дії бутового вірусу

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.

Схема дії вірусу

DIRСучасні 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 (CompanionViruses) 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-пpогpами 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. В класифікації вірусів Dr.Solomon’s присутні також “троянські програми” (TROJANS), котрі проводять шкідливі дії замість оголошених легальних функцій або наряду з ними. Вони не спроможні на самовідтворення і передаються тільки при копіюванні користувачем. Цікаве явище презентує собою поганий вірус – як результат порчі реального вірусу або просто погано написаний програмістом. Такий вірус нічого не може зробити – або “висне” при виконанні, або не може заражати інші файли. Інколи йде інший процес – вірус виконує непродумані дії, котрі ведуть до знищення інформації. Серед авторів вірусів нечасто зустрічаються погані програмісти. Всього на сьогоднішній день існують тисячі вірусів, але тільки в декількох десятках із них реалізовані оригінальні ідеї, інші є лише “варіаціями на тему”.

Висновок

В даній роботі я розглянула принцип дії і ознаки комп’ютерних вірусів.  Зокрема їхню дію на ПК, що показали певні результати. Так вірусні програми, які появилися першими, насправді не були шкідливими, а розповсюджувалися за допомогою локальної мережі і вибивали різні текстові повідомлення на ПК не шкодячи йому. В наші часи із 100% вірусів які існують в локальні мережі Internet тільки 12% вірусів є насправді небезпечними для ПК і її операційної системи. А саме «троянський кінь» який маскується під різними програми, не даючи цим виявити себе. Ранні ознаки зараження дуже тяжко виявити, але коли вірус переходить в активну фазу, тоді легко помітити зміни.

Практична частина

Для того, щоб виявити віруси спочатку потрібно ознайомитись із їх ознаками і принципами дій. Потім потрібно встановити антивірусну програму і почати сканувати. Стикнувшись з даною проблемою, ми використали таки антивірусні програми, як антивірус AVAST, «Доктор Веб», антивірус Касперського. . Певні віруси нам вдалося виявити і видалити. З вірусами-троянами нам прийшлося попрацювати дещо старанніше. Ще ми використовували Malwarebytes Anti-malware. Загалом, було виявлено 13 заражених файлів.

Посилання:

1. VX Heaven
2. Інформатика: Навчальний посібник для 10-11 кл. Зарецька І.Т. Колодяжний Б.Г
3. Журнал “Компьютерное обозрение” №35(108) за 10 жовтня 1997 рік.
4. Тхір І.Л, Галушка ВП. Юзьків А.В.Посібник користувача ПК.
5. http://www.kurs-pk.com/windows/virus/virus1.html
6. http://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF'%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D0%B9\_%D0%B2%D1%96%D1%80%D1%83%D1%81