Комп'ютерні віруси. Антивірусні програми

Комп’ютерний вірус

- Комп’ютерний вірус – це спеціально створена програма, або сукупність машинного коду, яка здатна розмножуватись і, як правило, виконує на ПК певні деструктивні дії.

- За способом зараження більшість комп'ютерних вірусів можна підрозділити на два класи: файлові та бутові віруси. Розглянемо коротко механізми їх дії.

Файлові віруси

- 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.

Вірус VIENNA

- Один із перших найбільш примітивних файлових 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

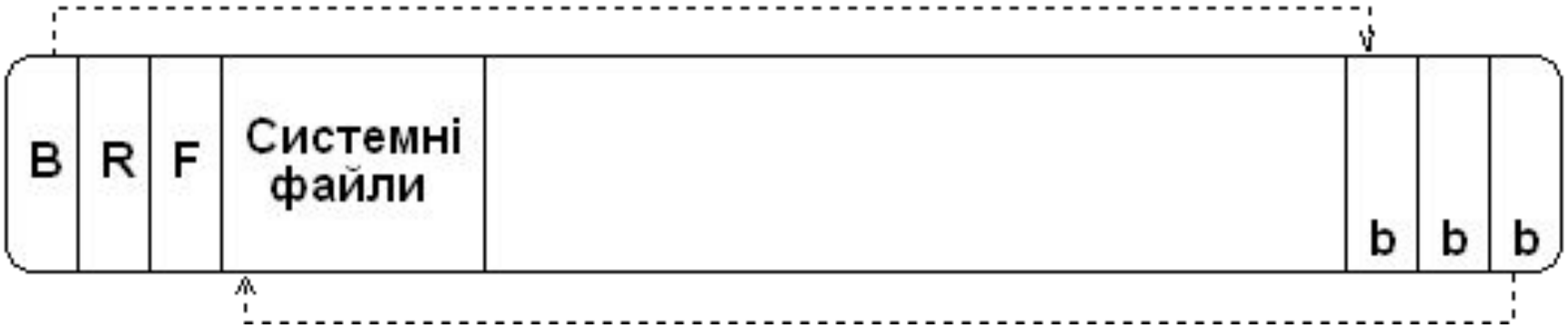
- Останнім часом з'явились віруси, які впроваджують себе до файлу, що заражається окремими "плямами". При запису у середину файлу вірус інколи знаходить "порожні" місця і приміщує туди своє тіло, не змінюючи довжину жертви. У більшості випадків довжина інфікованого файлу збільшується на деяку величину, 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).

Doctor Wett

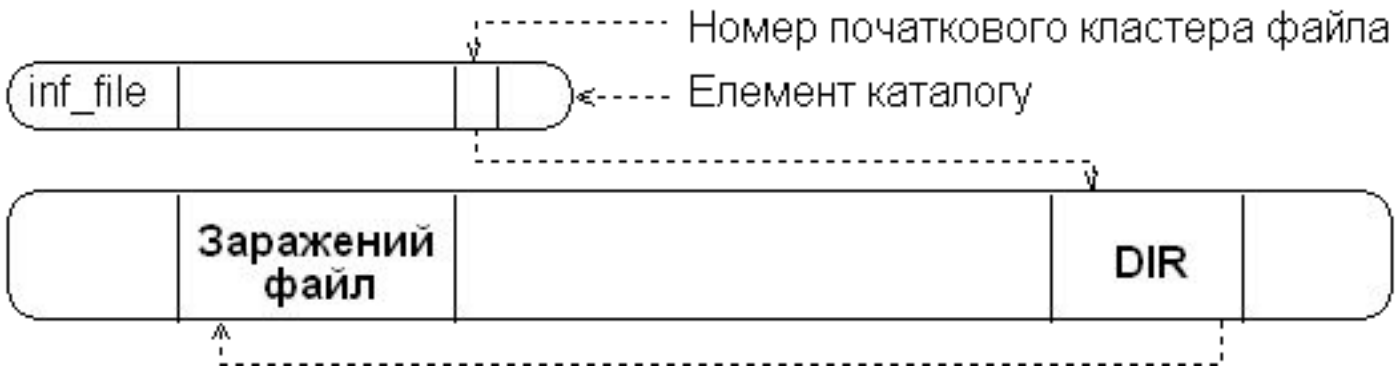
- Перші комп’ютерні віруси з’явились на початку 80-х років. Програма Doctor Wett (спрощено Dr.WEB) один з кращих в світі антивірусів, розроблених вперше для DOS у 1992 р. російським програмістом Ігорем Даніловим та керованою ним компанією “Діалог-Наука” (Санкт Петербург). В другій половині 90-х розроблено також версії з графічним інтерфейсом для Windows. Від самого початку свого існування по сьогоднішній день програма залишається одним зі лідерів серед антивірусних програм продуктів. Вона неодноразово, отримувала нагороди від Visus Bulettin за 100% виявлення вірусів різних типів.

Бутові віруси

- Бутові віруси заражають Boot-сектор вінчестера або дискет. Механізм зараження цими вірусами представлений на рис. 2. 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. Схема дії вірусу DIR приводиться на рис. 3.

- 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.
- 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.

Віруси-супутники

- 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).

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-код4), який, переміщуючись по екрану, відбивається від його границь та рамок, утворених символами псевдографіки.

Ознаки зараження вірусом

- Уповільнення роботи комп’ютера.
- Затримка при виконанні програм.
- Зміни в файлах.
- Зміна дати модифікації файлів без причини.
- Помилки при інсталяції та запуску WINDOWS.
- Неспроможність зберігати документи Word в інші каталоги.
- Погана робота дисків.
- Зникнення файлів.
- Неспроможність завантажити комп’ютер.
- Неспроможність завантажити файли.
- Незрозумілі системні повідомлення, музикальні ефекти і т.д.
- Неспроможність нормально працювати.

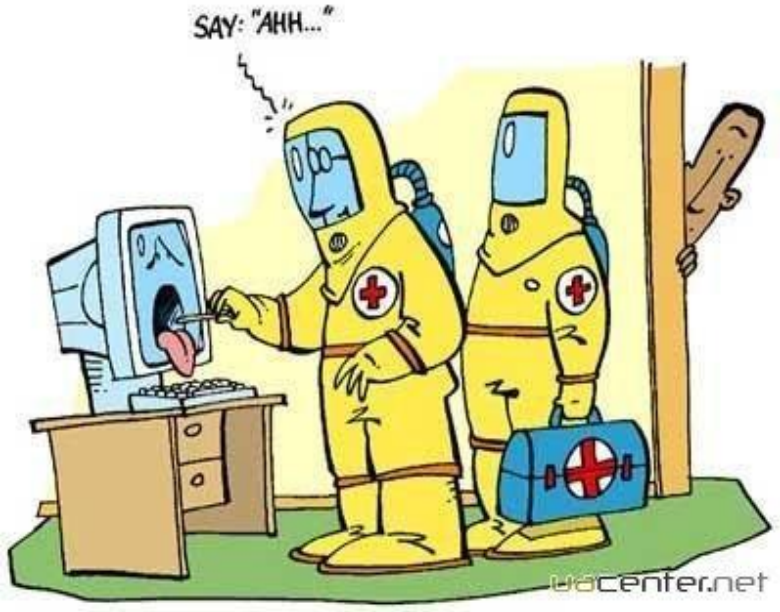
Антивірусні програми

Тип антивірусної програми	Принцип дії
Детектори	Виявляють файли, заражені одним з відомих вірусів
Лікарі (фаги)	"Лікують" заражені програми, або диски, Вилучають із заражених програм код вірусу, тобто відновлюють програму в тому стані в якому вона була до зараження вірусом
Ревізори	Спочатку запам'ятовують відомості про стан програм і системних областей дисків, а потім а потім порівнюють їх стан з вихідним. При виявленні невідповідності повідомляють про нього.
Фільтри	Завантажуються резидентно в оперативну пам'ять, перехоплюють ті звернення до системи, які використовуються вірусами для розмноження і нанесення шкоди, і повідомляють про них. Можна дозволити або заборонити виконання даної операції.

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

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):



Презентацію підготувала

- Учениця 9-А класу
- Хрипко Анна