ВІРУСИ ТА АНТИВІРУСИ

Комп'ютерний вірус (КВ) – це програма, здатна створювати свої копії (не обов'язково повністю співпадаючі з оригіналом), впроваджувати їх у різні об'єкти або ресурси комп'ютерних систем, мереж і робити певні дії без ведена користувача.

Своя назву *КВ* одержавши за деяка подібність із біологічним вірусом. Наприклад, у зараженій програмі самовідтворюється інша програма-вірус, а інфікована програма може тривалий година працювати без помилок, як у стадії інкубації.

Програма, усередині якої перебуває вірус, називається *зараженої (інфікованої)* програмою.

Коли інфікована програма починає роботові, ті спочатку керування одержує вірус. Він заражає інші програми, а також виконує заплановані деструктивні дії. Для маскування своїх дій вірус активізується не завжди, а лише при виконанні певних розумів (витікання деякого години, виконання певного числа операцій, настання деякої дати або дня тижня і т.д.). Після того, як вірус виконає потрібні йому дії, він передає керування тій програмі, у якій він перебуває. Зовні заражена програма може працювати так саме, як і звичайна програма. Подібно сьогоденням вірусам КВ ховаються, розмножуються й шукають можливості перейти на інші ЕОМ.

Незважаючи на широку поширеність антивірусних програм, віруси продовжують плодитися. У середньому в день з'являється близько 300 нових різновидів.

6.1 Функціонування

Різні віруси виконують різні дії:

Виводять на екран текстові повідомлення, що заважають поздоровлення, політичні гасла, фрази із претензією на юмор и т.д.);

Створюють звукові ефекти (гімн, гама, популярна мелодія);

Створюють відео ефекти (перевертають або зрушують екран, імітують землетрус, викликають обпадання букв у тексті, виводять картинки і т.д.);

Сповільнюють роботу ЕОМ, поступово зменшують обсяг вільної оперативної пам'яті;

Збільшують спрацювання устаткування (наприклад, головок дисководів);

Викликають відмова окремих пристроїв, зависання або перезавантаження комп'ютера й крах роботи всієї ЕОМ;

Знищують FAT, форматують жорсткий диск, стирають BIOS, знищують або змінюють дані, стирають антивірусні програми;

Здійснюють наукове, технічне, промислове й фінансове шпигунство;

Виводять із ладу системи захисту інформації і т.д.

Головн небезпек кодов, що самовоспроизводящихся, заключается в том, что программы-вирусы начинают жить собственной жизнью, практически не зависящей от Так само, як у ланцюговій реакції в ядерному реакторі, запущений процес важко зупинити.

6.2 Симптоми вірусного зараження ЕОМ:

Затримка роботи деяких програм

Збільшення розмірів файлів (особливо виконуваних)

Поява не існуючих раніше «дивних» файлів

Зменшення обсягу доступної оперативної пам'яті (у порівнянні зі звичайним режимом роботи)

Раптово виникаючі різноманітні відео й звукові ефекти

Поява збоїв у роботі ОС (у т.ч. зависання)

Запис інформації на диски в моменти часу, коли цього не повинне відбуватися

Припинення роботи або неправильна робота програм, що раніше нормально функціонували.

6.3 Класифікація вірусів

Існує велика кількість різних класифікацій вірусів:

По середовищу проживання:

Мережні – поширюються по мережах (Melissa).

Файлові – інфікують, що виконуються файли з розширеннями .exe, .com. Також до цього класу ставляться макровіруси, які заражають неисполняемые файли (наприклад, в MS WORD або в MS EXCEL).

Завантажувальні – впроваджуються в завантажувальний сектор диска (Boot-Сектор) або в сектор, що містить програму завантаження системного диска (Master Boot Record - MBR). Деякі віруси записують своє тіло у вільні сектори диска, позначаючи їх в FAT як «погані».

Файлово-Завантажувальні – здатні заражати й завантажувальні сектори й файли.

По способу зараження:

Резидентні – залишають в оперативній пам'яті свою резидентну частину, яка потім перехоплює обіги програм до ОС і впроваджується в них. Свої деструктивні дії вірус може повторювати багаторазово.

Нерезидентні – не заражають оперативну пам'ять і проявляють свою активність лише однократно при запуску зараженої програми.

По ступеню небезпеки:

Безпечні – наприклад, на екрані з'являється повідомлення: «Прагну чучу». Якщо набрати на клавіатурі слово «чуча», то вірус тимчасово «заспокоюється».

Небезпечні – знищують частина файлів на диску.

Дуже небезпечні – самостійно форматують жорсткий диск. (CIH – активізується 26 числа кожного місяця й здатний знищувати дані на жорсткому диску й в BIOS).

По особливостях алгоритму:

Віруси-Компаньйони – створюють для exe-файлів нові файли-супутники, що мають те ж ім'я, але з розширенням com. Вірус записується в com-файл і ніяк не змінює однойменний exe-файл. При запуску такого файлу ОС першим виявить і виконає com-файл, тобто вірус, який потім запустить і exe-файл.

Паразитичні – змінюють уміст дискових секторів або файлів.

Репликаторы (хробаки) – поширюються в мережі. Вони проникають на згадку комп'ютера з мережі, обчислюють мережні адреси інших комп'ютерів і розсилають по цих адресах свої копії. Хробаки зменшують пропускну здатність мережі, сповільнюють роботу серверів. Можуть розмножуватися без впровадження в інші програми й мати

«начинку» з комп'ютерних вірусів. («Хробак Морриса» наприкінці 80-х паралізував кілька глобальних мереж у США).

Невидимки (стелс) – маскують своя присутність в ЕОМ, їх важко виявити. Вони перехоплюють обіги ОС до уражених файлів або секторів дисків і «підставляють» незаражені ділянки файлів.

Мутанти (примари, поліморфні віруси, полиморфики) – їх важко виявити, тому що їхні копії практично не містять повністю співпадаючих ділянок коду. Це досягається тим, що в програми вірусів додаються порожні команди (сміття), які не змінюють алгоритм роботи вірусу, але утрудняють їхнє виявлення. (Onehalf – локальні «епідемії» його виникають регулярно).

Макро-Віруси – використовують можливості макромов, вбудованих у системи обробки даних (Word, Excel).

«Троянські коні» – маскуються під корисну або цікаву програму, виконуючи під час свого функціонування ще й руйнівну роботу (наприклад, стирає FAT) або збирає на комп'ютері інформацію, що не підлягає розголошенню. Не мають властивість самовідтворення.

По цілісності:

Монолітні – програма вірусу - єдиний блок, який можна виявити після інфікування.

Розподілені – програма розділена на частині. Ці частини містять інструкції, які вказують комп'ютеру, як зібрати їх воєдино, щоб відтворити вірус.

6.4 Антивірусні програми

Для боротьби з вірусами розробляються антивірусні програми. Говорячи медичною мовою, ці програми можуть виявляти (діагностувати), лікувати (знищувати) віруси й робити щеплення «здоровішим» програмам.

Однак слід зазначити, що не існує антивірусів, що гарантують стовідсотковий захист від вірусів. Таких систем не існує, оскільки на будь-який алгоритм антивірусу завжди можна запропонувати контр-алгоритм вірусу, невидимого для цього антивірусу (зворотне, на щастя, теж вірно: на будь-який алгоритм вірусу завжди можна створити

антивірус). Більше того, неможливість існування абсолютного антивірусу була доведена математично на основі теорії кінцевих автоматів, автор доказу - Фред Коэн.

6.4.1. Характеристика

Якість антивірусної програми визначається по наступних позиціях, наведених у порядку убування їх значимості.

Надійність і зручність роботи - відсутність зависань антивірусу й інших технічних проблем, що вимагають від користувача спеціальної підготовки.

Це найбільш важливий критерій, оскільки навіть абсолютний антивірус може виявитися пошукам, якщо він буде не в змозі довести процес сканування до кінця - зависне й не перевірить частина дисків і файлів і, таким чином, залишить вірус непоміченим у системі. Якщо ж антивірус вимагає від користувача спеціальних знань, то він також виявиться пошукам, більшість користувачів просто проігнорують повідомлення антивірусу.

Ну а якщо антивірус буде надто часто ставити складні запитання рядовому користувачеві, те, швидше за все, користувач перестане звертатися до такого антивірусу.

Якість виявлення вірусів усіх розповсюджених типів, сканування усередині файлів документів/таблиць (MS Word, Excel, Office), упакованих і архівіруваних файлів. Відсутність "неправильних спрацьовувань". Можливість лікування заражених об'єктів.

Будь-який антивірус пошук, якщо він не в змозі ловити віруси або робить це не цілком якісно. Тому якість детектирования вірусів є другим по важливості критерієм "якості" антивірусної програми. Однак якщо при цьому антивірус із високою якістю детектирования вірусів викликає велика кількість неправильних спрацьовувань, те його рівень корисності різко падає, оскільки користувач змушений або знищувати незаражені файли, або самостійно робити аналіз підозрілих файлів, або звикає до частих неправильних спрацьовувань - перестає звертати увагу на повідомлення антивірусу й у результаті пропускає повідомлення реальному вірусі.

Многоплатформность антивірусу є наступним пунктом у списку, оскільки тільки програма, розрахована на конкретну операційну систему, може повністю використовувати функції цієї системи. "Нерідні" же антивіруси часто виявляються непрацездатними, а іноді навіть руйнівними.

Можливість ***перевірки файлів на лету*** також є досить важливою рисою антивірусу. Моментальна й примусова перевірка прихожих на комп'ютер файлів, що й вставляються дискет є практично стовідсотковою гарантією від зараження вірусом.

Наступним по важливості критерієм є ***швидкість роботи***. Якщо на повну перевірку комп'ютера антивірусу потрібно кілька годин, то чи навряд більшість користувачів будуть запускати його досить часто. При цьому повільність антивірусу зовсім не говорить про те, що він ловить вірусів більше й робить це краще, чим більш швидкий антивірус. У різних антивірусах використовуються різні алгоритми пошуку вірусів, один алгоритм може виявитися більш швидким і якісним, інший - повільним і менш якісним. Усе залежить від здатностей і професіоналізму розроблювачів конкретного антивірусу.

Наявність додаткових функцій і можливостей коштує в списку якостей антивірусу на останньому місці, оскільки дуже часто ці функції ніяк не позначаються на рівні корисності антивірусу. Однак ці додаткові функції значно спрощують життя користувача.

6.4.2. Види антивірусних програм:

Програми-Детектори (сканери) – розраховані на виявлення конкретних вірусів. Засновані на порівнянні характерної (специфічної) послідовності байтів (*сигнатур* або масок вірусів), що втримуються в тілі вірусу, з байтами програм, що перевіряються. Ці програми потрібно регулярно обновляти, тому що вони швидко застарівають і не можуть виявляти нові види вірусів. Якщо програма не зорієнтується детектором як заражена, це ще не виходить, що вона «здорова». У ній може бути вірус, який не занесений у базу даних детектора.

Програми-Доктори (фаги, дезінфектори) –не тільки знаходять файли, заражені вірусом, але й лікують їх, видаляючи з файлу тіло програми-вірусу. Полифаги – дозволяють лікувати велика кількість вірусів. Широко поширені програми-детектори, що одночасно виконують і функції програм-докторів. Приклади: AVP (автор Е. Касперский), Aidstest (Д. Лозинский), Doctor Web (І. Данилов).

Програми-Ревізори – аналізують поточний стан файлів і системних областей дисків і порівнюють його з інформацією, збереженої раніше в одному з файлів ревізора. При цьому перевіряється стан Boot-Сектору, FAT, а також довжина файлів, їх час створення,

атрибути, контрольні суми (підсумовування по модулю 2 усіх байтів файлу). Приклад такої програми – Adin f (Д. Бруківці).

Програми-Фільтри (сторожачи, монітори) – резидентні програми, які сповіщають користувача про всі спроби якої-небудь програми виконати підозрілі дії, а користувач ухвалює рішення щодо дозволу або заборони виконання цих дій. Фільтри контролюють наступні операції: відновлення програмних файлів і системної області дисків; форматування диска; резидентне розміщення програм в ОЗУ. Прикладом служить програма Vsafe. Вона не здатна знешкодити вірус, для цього потрібно використовувати фаги.

Програми-Иммунизаторы – записують у вакцинируемую програму ознаки конкретного вірусу так, що вірус уважає її вже зараженої, і тому не робить повторне інфікування. Ці програми найменш ефективні й морально застаріли.

6.4.3.Принцип роботи антивірусу

Говорячи про системи Майкрософт, слід знати, що звичайно антивірус діє за схемою:

пошук у базі даних антивірусного ПО сигнатур вірусів

якщо знайдений інфікований код у пам'яті (оперативної й/або постійної), запускається процес карантину, і процес блокується

зареєстрована програма звичайно видаляє вірус, незареєстрованна просить реєстрації й залишає систему вразливої

6.5 Заходи щодо захисту ЕОМ від зараження вірусами:

Оснащення ЕОМ сучасними антивірусними програмами й регулярне відновлення їх версій.

Установка програми-фільтра при роботі в глобальній мережі.

Перевірка дискети на наявність вірусів перед зчитуванням з дискет інформації, записаної на інших ЕОМ.

При переносі на свій ПК файлів в архівіруваному виді перевірка їх відразу після разархивации.

Захист своїх дискет від запису при роботі на інших ПК.

Створення архівних копій коштовної інформації на інших носіях інформації.

Не залишати дискету в дисководі при включенні або перезавантаження ПК, тому що можливе зараження завантажувальними вірусами. Наявність аварійної завантажувальної дискети, з якої можна буде завантажитися, якщо система відмовиться зробити це звичайним образом.

При установці великого програмного продукту спочатку перевірити всі дистрибутивні файли, а після інсталяції продукту повторно зробити контроль наявності вірусів.

6.6 Бази антивірусів

Для використання антивірусів необхідні постійні відновлення так званих баз антивірусів. Вони являють собою інформацію про віруси — як їх знайти й знешкодити. Оскільки віруси пишуть часто, те необхідний постійний моніторинг активності вірусів у мережі. Для цього існують спеціальні мережі, які збирають відповідну інформацію. Після збору цієї інформації проводиться аналіз шкідливості вірусу, аналізується його код, поведінку, і після цього встановлюються способи боротьби з ним. Найчастіше віруси запускаються разом з операційною системою. У такому випадку можна просто вилучити рядка запуску вірусу з реєстру, і на цьому в простому випадку процес може закінчитися. Більш складні віруси використовують можливість зараження файлів. Наприклад, відомі випадки, як якісь навіть антивірусні програми, будучи зараженими, самі ставали причиною зараження інших чистих програм і файлів. Тому більш сучасні антивіруси мають можливість захисту своїх файлів від зміни й перевіряють їх на цілісність по спеціальному алгоритму. Таким чином, віруси ускладнилися, як і ускладнилися способи боротьби з ними.

Зараз можна побачити віруси, які займають уже не десятки кілобайт, а сотні, а часом можуть бути й розміром у парі мегабайт. Звичайно такі віруси пишуть у мовах програмування більш високого рівня, тому їх легше зупинити. Але як і раніше існує погроза від вірусів, написаних на низкоуровневых машинних кодах на зразок асемблера. Складні віруси заражають операційну систему, після чого вона стає вразливою й неробочою. На жаль, за прогнозами, у найближчому майбутньому робота антивірусних

компаній сильно ускладниться у зв'язку з тим, що будуть сильніше поширюватися віруси із захистом від копіювання.