Комп’ютерні віруси

Вважається, що термін "комп'ютерний вірус" впершезастосував співробітник Лехаїського університету (США) Ф. Коен на конференції з безпеки інформації в 1984 р. Комп'ютерні віруси також володіють здібністю до самовідтворення з наступним впровадженням копій вірусу у файли, системні області комп'ютера або навіть на інший комп'ютер по мережі. При цьому дублікати також зберігають здібність до подальшого розповсюдження. Як правило, віруси володіють якою-небудь деструктивною дією, хоча це і не є обов'язковою умовою. Здібність до самовідтворення треба розуміти дуже широко. Різні примірники одного вірусу не тільки не зобов'язані повністю збігатися, але можуть, навіть не мати жодного загального байта (йдеться про так звані складнополіморфнівіруси).

Класифікація вірусів

Класифікація за метою дії

- Завантажувальні (бутові) віруси - віруси, що заражають завантажувальні сектори дискет і жорстких дисків. Існують бутові віруси, завантажувальні сектори дискет, інші заражають - ще і завантажувальні сектори вінчестерів, деякі - заражають головний завантажувальний сектор вінчестера (MBR). Часто віруси "всеїдні" і заражають і те, і інше.
- Файлові віруси - заражають виконувані файли. Крім того, до файлових відносяться так звані macro-віруси - файлові віруси, що заражають файли деяких систем документообігу, наприклад, MS Office, AmiPro ін. Такі системи мають вбудовані макро - мови (VBA, VB). Ці мови володіють достатніми можливостями, щоб проводити практично всі операції, необхідні вірусу. Для розмноження в середовищі MS Office такі віруси використовують файл шаблону за умовчанням normal.dot.
- Віруси, що вражають код BIOS комп'ютера.
- Скрипт - віруси створюються на мові сценаріїв VBS, розробленій Microsoft. Така мова виконується інтерпретатором Windows, крім того, веб - браузером MS Internet Explorer. Подібні віруси можуть видаляти файли на жорсткому диску, змінювати настройки системи, запускати троянських коней і ін. Якщо у веб - браузері неправильно настроєний розділ «Безопасность», то загроза інфікування такими вірусами існує при відвідуваннях веб - сторінки, що містять шкідливий VBS - скрипт.
- Мережеві черв'яки - це шкідницькі комп'ютерні програми, які можуть створювати свої копії на одному і тому ж комп'ютері чи ж копіювати себе на інші комп'ютери мережі, використовуючи найчастіше систему електронної пошти. Розсилка черв'яків за адресами адресної книги поштових клієнтів призводить до вибухоподібного зростання повідомлень, що пересилаються, що може привести до перевантаження каналів і відмови в обслуговуванні.
- Троянські коні - це програми, які маскуються під які-небудь корисні застосування (наприклад, утиліти або навіть антивірусні програми), але при цьому завдають різні руйнівні дії. Трояни не вбудовуються в інші файли і не володіють здібністю до власнодублювання. В порівнянні з іншими типами вірусів «троянські коні» мало поширені, оскільки після запуску вони або знищують себе разом з рештою даних на диску, або знищуються самим постраждалим користувачем.
- Backdoor-програми - утиліти прихованого адміністрування аналогічні троянським коням, але на відміну від останніх, самі не виконують активних дій, а тільки відчиняють доступ на комп'ютер зловмиснику.

Класифікація за властивостями вірусів

- Віруси, що маскуються (Stealth). Видів маскування безліч, але всі вони засновані на перехопленні вірусами переривань BIOS і операційної системи. Перехопивши переривання, віруси контролюють доступ до заражених об'єктів. Наприклад, при прогляданні зараженого об'єкту, вони можуть "підсунути" замість нього здоровий. Крім того, віруси спотворюють інформацію BIOS (наприклад, повертають невірне значення довжини файлу, приховуючи свою присутність в ньому). Для більшості антивірусних програм віруси, що використовують стелс - технологію, є серйозною проблемою. Винятком є програми-ревізори дисків (наприклад, AdInf).
- Поліморфні віруси. Аналіз вірусів полягає у виділенні в них сигнатур (послідовності байт, специфічної (у ідеалі - унікальної) для конкретної програми) і подальшому пошуку в потенційних об'єктах вірусної атаки. Поліморфні віруси шифрують свій код. Мета такого шифрування достатньо очевидна: маючи заражений і оригінальний файли, і, отже, маючи можливість виділити вірус "в чистому вигляді", не представляється можливим проаналізувати його код за допомогою звичайного дизасемблювання. Розшифровка проводиться самим вірусом вже безпосередньо під час виконання. При цьому можливі самі різні варіанти: вірус може розшифрувати себе всього відразу, а може виконувати таку розшифровку по частинах, може знов шифрувати вже відпрацьовані ділянки і т.д. (причому іноді не тим способом, яким вони були зашифровані раніше). Проте зашифровані віруси обов'язково містять деякий незашифрований фрагмент - розшифровщик (або його частка). По ньому можна побудувати сигнатуру такого вірусу і далі вже боротися з ним звичайними способами. Ситуація змінилася, коли були розроблені алгоритми, що дозволяють не тільки шифрувати код вірусу, але і змінювати розшифровщики - кожна нова копія вірусу містить новий розшифровщик, який може в кожному біті відрізнятися від розшифровщика, що створив похідні копії. Навіть з простих комбінаторних міркувань ясно, що розшифровщиків, довжина яких звичайно обмежена, не може бути нескінченно багато. Але якщо їх всього лише два-три трильйона, то ясно, що задача перебору всіх можливих не стоїть. Віруси, що використовують описану технологію, одержали назву поліморфних.
- Резидентні віруси відрізняються від нерезидентних тим, що після запуску інфікованої програми вони залишаються в оперативній пам'яті комп'ютера.

Типи антивірусних засобів:

- Сканери - поліфаги. Пошук вірусів в простому випадку зводиться до пошуку їх сигнатур. Після виявлення вірусу в тілі програми 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 і т. д. В більшості випадків поліфаг здатний благополучно видалити вірус і відновити працездатність зіпсованих програм. Але необхідно добре розуміти, що це можливо не завжди. Сучасні антивірусні програми містять засоби евристичного аналізу, що дозволяють розпізнавати деструктивний код в нових, ще не відомих поліфагу вірусах.
- Сторожа - невеликі резидентні програми, перевіряючі завантажувані в пам'ять файли на предмет знаходження в них сигнатур вірусів. Перевага - швидке

виявлення вірусів. Недолік - сильне завантаження систем і зниження їх продуктивності.

- Ревізори - програми, у функції яких входить антивірусна перевірка шляхом контролю властивостей файлів (розміру, дати і часу створення / зміни, контрольної суми і ін.). При цьому виконується порівняння властивостей файлів з їх первинними значеннями (дуже важливо, щоб вони не належали вже зараженим файлам). Внаслідок перевірки користувачу виводиться список файлів із зміненими властивостями, і користувач вирішує, які з файлів змінив він сам, а які можливо заражені. Часто ревізори працюють в тандемі зі сканерами - поліфагами і автоматично передають їм на перевірку файли із зміненими властивостями.
- Антивірусні вакцини, які використовувалися для обробки файлів і завантажувальних секторів. Вакцини бувають пасивними (приклад такої вакцини описаний нижче) і активними. Активна вакцина, "заражаючи" файл, подібно до вірусу, оберігає його від будь-якої зміни і у ряді випадків здатна не тільки виявити сам факт зараження, але і вилікувати файл. Пасивні вакцини використовувалися (тепер це вже велика рідкість) для запобігання зараження файлів деякими вірусами, що використовують прості ознаки їх зараженості - "дивні" час або дата створення, певні символьні рядки і ін. Нині вакцинація широко не застосовується.

Крім того, існують спеціальні додаткові пристрої (звичайно електронна плата із спеціалізованим процесором), що забезпечують досить надійний захист. Перевагою плати є незалежність від операційної системи і BIOS (які можуть бути заражені), а також практично відсутність використання ресурсів комп'ютера. Прикладом апаратних засобів антивірусного захисту може служити плата Sheriff.

Існує таке поняття як вірусна містифікація (Virus hoax) - помилкове попередження про нібито грізному вірусі, який насправді не існує. Наприклад, поступило по e-mail попередження про загрозу небезпечного вірусу, який записує своє тіло в один з файлів в каталозі Windows. В результаті багато користувачів помилково видалялицей необхідний для функціонування операційної системи файл.