Перші дослідження штучних конструкцій, які здатні до відтворення самих себе, проводились в середині минулого століття відомими вченими-математиками Джоном фон Нейманом і Норбертом Вінером. Звісно, в колишньому СРСР цьому питанню також приділялось достатньо уваги - вивчались самовідтворювальні кінцеві автомати.

Термін "комп'ютерний вірус" з'явився значно пізніше - офіційно вважається, що його вперше вжив співробітник Лехайського університету (США) Фред Коен у 1984 році на конференції. За означенням Коена,

**Комп'ютерний вірус - це програма, що володіє здатністю заражати інші програми, шляхом додавання до них своєї, можливо зміненої, копії**

Як бачимо, означення доволі неоднозначне. І чіткого формального визначення, що ж таке цей вірус, до сих пір немає.

Комп'ютерний вірус - одне з найцікавіших явищ, які можна спостерігати в результаті розвитку комп'ютерної техніки. Програми (які є лише послідовністю символів) набувають властивостей, що притаманні живим організмам - народжуються, розмножуються та вмирають.

Головна умова існування вірусів - універсальна інтерпретація інформації в обчислювальних системах. Один і той самий вірус у процесі зараження програми може сприймати її як дані, а в процесі виконання - вже як виконавчий код. Цей принцип було покладено в основу всіх сучасних комп'ютерних систем, які використовують архітектуру фон Неймана. Принципова відмінність вірусу від троянської програми полягає в тому, що вірус після попадання (з носієм) в комп'ютерну систему існує автономно і в процесі свого функціонування заражає (інфікує) програми.

Фізична структура вірусу є доволі простою. Він складається з голови та тіла (хвоста). Голова - це та частина коду вірусу, що виконується першою. Код тіла розміщується окремо від голови в коді зараженої програми. Якщо вірус складається лише з голови, то він називається несегментованим, з голови та тіла - сегментованим.

Для зараження файлів віруси використовують три основних способи (рис.16.2): запис з перекриттям (overwriting), запис на початку (prepending) та запис в кінці файлу (appending).

В першому випадку файл виявляється повністю зіпсованим, оскільки частину даних було затерто вірусом. Такі віруси зустрічаються вкрай рідко. При спробі відкрити заражений файл відбувається зараження ще одного файлу. Коли вірус записує себе на початку файлу, при його відкритті першим запускається код вірусу, а потім програма-оригінал. Віруси, розміщені після основного коду, переміщають початок програми (рис.16.2) в кінець файлу, а на його місці ставлять команду переходу на початок завантаження (jmp). Тобто керування одразу передається вірусу, що переносить початок програми назад і дозволяє програмі запуститись.

З поняттям "комп'ютерний вірус" тісно пов'язане таке поняття, як сигнатура. Сигнатура - це фрагмент коду, який є у всіх копіях вірусу і тільки в них. Тобто, це є підписом вірусу, що однозначно визначає його присутність або відсутність у програмі.



Рис.16.2. Варіанти розміщення вірусу у коді програми

Наприкінці минулого століття з'явилось багато дискусій та публікацій про те, чи може людина заразитись комп'ютерним вірусом? І знаходились такі, що відверто в це вірили, ототожнюючи комп'ютерний вірус з, скажімо, вірусом грипу. Та доки людина є живим організмом, комп'ютерні віруси будуть загрожувати лише інформації на її комп'ютері, програмному чи апаратному забезпеченню, але ніяк не здоров'ю.

Звісно, людину можна заразити аналогом комп'ютерного вірусу, ввівши йому в підсвідомість певну шкідливу ідею, але це вже буде предметом вивчення для галузі нейролінгвістичного програмування (програмування людини на низькому рівні).

Типи вірусів. Ефекти. Для виявлення та видалення вірусу насамперед необхідно його однозначно класифікувати за обмеженим набором простих і вірних ознак, які не потребують глибокого аналізу заражених програм і елементів ОС. Існує неофіційна класифікація, в якій назва вірусу відображає ту чи іншу його властивість:

* 1) за місцем виявлення або розробки вірусу
* (Jerusalem - зниження швидкодії комп'ютера, додає 1813 байтів до com-файлів та багатократно заражає exe-файли. Vienna - зациклювання при завантаженні);
* 2) за змістом текстових рядків у коді вірусу (Vacsine - змінює розширення файлу);
* 3) за ефектом дії вірусу (Cascade - "випадання" букв на нижню стрічку екрану)
* 4) за довжиною вірусу або зростанням довжини файлу при зараженні, або за датою активації. (524, 648, 2000)

Зазначимо, що така класифікація є суто практичною і не може використовуватись антивірусними засобами для ідентифікації вірусу. Оскільки той самий вірус, наприклад Cascade також може мати іншу назву - 1701, бо додає 1701 байтів до com-файлів. Вірус CIH, відомий також як Чорнобиль, тому що вірус активувався 26 квітня - день катастрофи на

Чорнобильській АБС. А от вірус Frodo (розміщує в сектор завантаження день народження хоббіта Фродо з "Володаря перснів" Толкієна) має дуже багато назв:

* o 4096 або 4К - за кількістю доданих байтів до com- та exe-файлів;
* o 100-річний, оскільки додає 100 років до дати створення зараженого файлу;
* o Stealth - бо при наявності вірусу в пам'яті, зміна довжини файлів при зараженні не відображається.

Отже, лише за такими властивостями вірусів віднести їх до певного типу буде дуже складно. Як вирішили цю проблему розробники антивірусної продукції? Вони почали використовувати для класифікації три основні елементи:

* o класифікаційний код вірусу;
* o дескриптор вірусу - формалізований список основних властивостей;
* o сигнатуру вірусу.

Класифікаційний код вірусу складається із літерного префіксу, кількісної характеристики та літерного суфіксу. Префікс вказує на місце розміщення голови вірусу і складається із літер та цифр. Відповідно до цього розрізняють такі типи вірусів:

* o файлові - голова розміщується у com- та exe-файлах (бувають резидентними та нерезидентними, за аналогією із програмними закладками, див.р.15). Символи C та E використовуються в префіксі;
* o бутові (від "boot"- початкове завантаження) - голова вірусу розміщується в секторі завантаження або у блоці MBR. Символи B, R або M у префіксі;
* o пакетні - голова вірусу представляє собою рядок чи програму на мові керування завданнями ОС. Префікс J;
* o гібридні - володіють властивостями декількох типів.

Характеристика вірусу - це кількісно вимірювальна властивість, яка допускає просте визначення і розрізняється для більшості типів вірусів. Наприклад, для файлових вірусів як характеристика може використовуватись величина приросту довжини файлу про зараженні.

Суфікс використовується у разі, якщо два різних віруси мають однаковий префікс та характеристику.

Наприклад, вірус з кодовим позначенням RCE-1813 є бутовим, що інфікує com- та exe-файли, додаючи до них 1813 байт.

В процесі реалізації вірус викликає в комп'ютерній системі ряд ефектів, які однозначно стверджують про його присутність:

* o спотворення інформації у файлах або таблиці розміщення файлів (FAT);
* o імітація порушень в роботі апаратного забезпечення;
* o створення звукових і візуальних ефектів, наприклад, сигнали точного часу через кожну годину або віконечко з написом "Комп'ютер створено не для ігор!!!"
* o повідомлення неправдивого змісту про стан системи, що ускладнюють роботу користувача;
* o ініціювання помилок в програмах або ОС;
* o зчитування з пам'яті і переміщення в інше місце інформації.

Хробаки та рекламні системи Adware. Хробак - це програма, яка розповсюджується через комп'ютерну мережу і не залишає своєї копії на магнітному носії. Хробак використовує механізм підтримки мережі для визначення вузла, який може бути заражений. Потім за допомогою тих самих механізмів передає своє тіло або його частину на цей вузол і активізується, або чекає сприятливих умов. Найсприятливішим середовищем для розповсюдження хробака є мережа, де користувачі довіряють один одному. Найкращім способом захисту від програм-хробаків є створення умов для неможливості несанкціонованого доступу до мережі.

У вірусу і хробака є спільною здатність до відтворення самих себе. Хробак копіює себе при першій нагоді. На відміну від вірусу, хробаку не потрібен носій.

Хробак може поширювати себе за допомогою пошти, ICQ чи інших засобів комунікації. Автори вірусів останнім часом почали все частіше використовувати програми, які самі по собі не є шкідливими, але залишають в системі троянську програму або завантажують її з Інтернету. Такі програми часто застосовують і для встановлення без відома користувача так званих Adware та Pornware програм, які не є вірусами, проте збирають інформацію про користувача. Adware - це програми, що відображають рекламу, іноді банери, без відома та згоди користувача. Pornware - програми, що з'єднуються із платними сайтами "для дорослих" також без відома та згоди користувача.

Жадібні програми (greedy programs). Вони намагаються монополізувати який-небудь ресурс, не даючи іншим програмам можливості використати його. Безпосередній атаці в більшості випадків піддаються такі об'єкти системи, як процесор, оперативна пам'ять, пристрої вводу-виводу.

Критична ситуація може виникнути тоді, коли "жадібна" програма виконує нескінчений цикл. Оскільки в багатьох ОС час використання процесора для однієї програми є обмеженим і контролюється системою, то "жадібна" програма може перехоплювати асинхронне до основної програми повідомлення про закінчення операцій вводу-виводу і посилати запит на новий ввід. Так можна досягти зациклення без можливості втручання ОС. Такі атаки називають також асинхронними.

Інший варіант "жадібної" програми - захоплення дуже великої ділянки оперативної пам'яті. Це є можливим, наприклад, при послідовному розміщенні в ОП великого обсягу даних, що надходять з зовнішнього носія (забивання пам'яті).

У галузі вірусів необхідно відзначити, що в 2004 році вперше з'явились загрози безпеці мобільних пристроїв. В червні був створений перший вірус для мобільних телефонів Саbir. Він представляв собою першу спробу - чи можливо взагалі заразити ПЗ мобільного телефону? Виявилось, що так. Тоді в липні з'явились вірус Duts та троянська програма Вrador, орієнтовані на платформу РоcketРС. Оскільки засоби захисту мобільних пристроїв є досить слабкими, то в недалекому майбутньому конфіденційній інформації на них буде загрожувати істотна небезпека.