Комп'ютерні віруси

Типи комп'ютерних вірусів розрізняються між собою по наступних основних ознаках:

- середовище незаселеного;
- спосіб зараження.

Під «середовищем незаселеного» розуміються системні області комп'ютера, операційні системи або додатки, в компоненти (файли) яких упроваджується код вірусу. Під «способом зараження» розуміються різні методи упровадження вірусного коду в об'єкти, що заражаються.

По середовищу незаселеного віруси можна розділити на:

- файлові;
- завантажувальні;
- макро;
- скриптові;
- шкідливих програм.

Файлові віруси

Файлові віруси при своєму розмноженні тим або іншим способом використовують файлову систему якої-небудь (або яких-небудь) операційної системи.

Вони:

- різними способами упроваджуються у виконувані файли (найпоширеніший тип вірусів);
- створюють файли-двійники (компаньйон-віруси);
- створюють свої копії в різних каталогах;
- використовують особливості організації файлової системи (link-віруси).

Завантажувальні віруси

- Файлові віруси
- За способом зараження файлів віруси діляться на:
- перезаписуючі (overwriting);
- паразитичні (parasitic);
- віруси-компаньйони (companion);
- віруси-посилання (link);
- віруси, об'єктні модулі, що заражають (OBJ);
- віруси, бібліотеки компіляторів, що заражають (LIB);
- віруси, початкові тексти програм, що заражають.

- Overwriting

Вірус записує свій код замість коду файлу, що заражається, знищуючи його вміст. Природно, що при цьому файл перестає працювати і не відновлюється.

- Parasitic

Віруси, які при розповсюдженні своїх копій обов'язково записуються в початок файлів, в кінець файлів і в середину файлів або вірусів, що не мають «точки входу», залишаючи самі файли при цьому повністю або частково працездатними.

- Companion

Це віруси, що не змінюють файлів, що заражаються. Алгоритм роботи цих вірусів полягає в тому, що для файлу, що заражається, створюється файл-двійник, причому при запуску зараженого файлу управління одержує саме цей двійник, тобто вірус. Можливо існування і інших типів вірусів-компаньйонів, що використовують інші оригінальні ідеї або особливості інших операційних систем. Існують віруси, які жодним чином не пов'язують свою присутність з яким-небудь виконуваним файлом. При розмноженні вони всього лише копіюють свій код в які-небудь каталоги дисків в надії. Link-віруси також не змінюють фізичного вмісту файлів, проте при запуску зараженого файлу «примушують» Ос виконати свій код.

Макро-віруси

Завантажувальні віруси записують себе або в завантажувальний сектор диска (boot-сектор), або в сектор, системний завантажувач вінчестера (Master Boot Record), що містить, або міняють покажчик на активний boot-сектор.

Даний тип вірусів був достатньо поширений в 1990-х, але практично зник з переходом на 32-бітові операційні системи і відмовою від використовування дискет як основного способу обміну інформацією. Теоретично можливо поява завантажувальних вірусів, що заражають CD-диски і USB-флешек, але на даний момент такі віруси не знайдені.

Скриптові віруси

Багато табличних і графічних редакторів, систем проектування, текстові процесори мають свої макро-мови для автоматизації виконання дій, що повторюються. Ці макро-мови часто мають складну структуру і розвинутий набір команд. Макро-віруси є програмами на макро-мовах, вбудованих в такі системи обробки даних. Для свого розмноження віруси цього класу використовують можливості макро-мови і при їх допомозі переносять себе з одного зараженого файлу (документа або таблиці) в інші.

Найбільше розповсюдження отримали макро-вирусы для Microsoft Office (Word, Excel і PowerPoint), що бережуть інформацію у форматі OLE2 (Object Linking and Embedding). Віруси в інших додатках достатньо рідкісні.

Комп'ютерні віруси

Слід зазначити також скрипт-віруси, що є підгрупою файлових вірусів. Дані віруси, написані на різних скрипт-мовах (VBS, JS, BAT, PHP і т.д.). Вони або заражають інші скрипт-програми (командні і службові файли MS Windows або Linux), або є частинами багатокомпонентних вірусів. Також, дані віруси можуть заражати файли інших форматів (наприклад, HTML), якщо в них можливо виконання скриптів.

Шкідливі програми

До шкідливого програмного забезпечення відносяться мережні черв'яки, класичні файлові віруси, троянські програми, хакерскі утиліти і інші програми, що завдають явної шкоди комп'ютеру, на якому вони запускаються на виконання, або іншим комп'ютерам в сіті.

Величезний вплив на сучасну вірусологію надали всесвітні епідемії, викликані наступними мережними і поштовими черв'яками: Lovesan, Sobig, Swen і Sober. Кожний з них звів в ранг еталона власні відмінні риси (можуть створювати зомбі-машини, прагнення до видалення інших черв'яків із заражених машин, розсилка себе у вигляді архівів, закритих паролем архівів з вказівкою пароля в тексті листа або у вигляді картинки, відмова від пересилки свого тіла по електронній пошті і відправка натомість в листі посилання на веб-сайт або на заражений раніше комп'ютер, організація спам-розсилки,...), всі з яких активно використовуються в даний час новими вірусами і продовжуватимуть використовуватися в досяжному майбутньому.

Мережні черв'яки і класичні файлові віруси

До даної категорії відносяться програми, поширюючі свої копії по локальних і/або глобальних мережах з метою:

- проникнення на видалені комп'ютери і запуску своєї копії ;
- подальшого запуску свого коду при яких-небудь діях користувача;
- подальшого упровадження в інші ресурси комп'ютера.
- подальшого розповсюдження на інші комп'ютери в мережі.

Більшість відомих черв'яків розповсюджується у вигляді файлів. Деякі черв'яки (так звані «бесфайлові» або «пакетні черв'яки») розповсюджуються у вигляді мережних пакетів, проникають в пам'ять комп'ютера і активізують свій код.

Для проникнення на видалені комп'ютери і запуску своєї копії черв'яки використовують різні методи: соціальний інжиніринг (текст електронного листа, що закликає відкрити вкладений файл), недоліки в конфігурації мережі, помилки в службах безпеки операційних систем і додатків.

Деякі черв'яки володіють також властивостями інших різновидів шкідливого програмного забезпечення.

Троянські програми

В дану категорію входять програми, здійснюючі різні несанкціоновані користувачем дії: збір інформації і її передачу зловмиснику, її руйнування або зловмисну модифікацію, порушення працездатності комп'ютера, використовування ресурсів комп'ютера в непристойній меті.

Окремі категорії троянських програм завдають збитку видаленим комп'ютерам і сітям, не порушуючи працездатність зараженого комп'ютера (наприклад, троянські програми, розроблені для масованих DoS-атак на видалені ресурси мережі).

Хакерські утиліти і інші шкідливі програми

До даної категорії відносяться:

- утиліти автоматизації створення вірусів, черв'яків і троянських програм (конструктори);
- програмні бібліотеки, розроблені для створення шкідливого ПО;
- хакерскі утиліти утаєння коду заражених файлів від антивірусної перевірки (шифрувальники файлів);
- «злі жарти», що утрудняють роботу з комп'ютером;
- програми, що повідомляють користувачу явно помилкову інформацію про свої дії в системі;
- інші програми, тим або іншим способом навмисно завдаючі прямого або непрямого збитку даному або видаленим комп'ютерам.