

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 скриптові і 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.

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.

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-віруси 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 багатокomпонентних вірусів. Також, дані віруси можуть заражати файли інших форматів (наприклад, HTML), якщо в них можливо виконання скриптів.

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, використання 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;
- хакерські 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 завдаючи прямого або непрямого збитку даному або видаленим комп'ютерам.