РЕФЕРАТ

на тему

«Комп’ютерні віруси. Класифікація»

2010-06-15

Комп’ютерний вірус – спеціально написана невелика за розміром програма (тобто деяка сукупність виконуваного коду, призначена для заподіяння руйнівних дій ). Вона може «приписувати» себе до інших програм («заражати» їх ), створювати свої копії і вбудовувати їх у файли, системну ділянку комп’ютера тощо,а також виконувати різноманітні небажані дії.

Комп’ютерні віруси класифікуються на :

1. Мережні які поширюються комп’ютерними мережами.
2. Файлові які вбудовуються у виконувані файли (найбільш поширений тип вірусів), або створюють файли – двійники (компаньйон – віруси ), або використовують особливості організації файлової системи (link віруси )
3. Завантажувальні які записують себе або в завантажувальний сектор диска (bootсектор),або сектор, який містить системний завантажник вінчестера (Master Boot Record ), або змінюють покажчик на активний bootсектор
4. Файлово – завантажувальні які завантажують як файли, так і завантажувальні сектори дисків
5. Резидентний вірус який у разі інфікування комп’ютер залишає в оперативній пам’яті свою резидентну частину, що потім перехоплює обертання ОС до об’єктів зараження і вбудовується в них. Цей вид віруса міститься в пам’яті і є активним аж до вимикання комп’ютера або перезавантаження ОС
6. Нерезедентний вірус який зберігає свою активність обмежений час
7. Безпечні віруси яких вплив обмежується зменшенням вільної пам’яті на диску та графічними, звуковими й іншими ефектами
8. Небезпечні які можуть призвести до серйозних збоїв у роботі комп’ютера
9. Дуже небезпечні в яких в алгоритм роботи явно закладено дії, що можуть спричинити втрату програм, знищити дані тощо
10. Найпростіші віруси (паразитичні) які змінюють уміст файлів і секторів диска ; їх можна достатньо легко виявити і знищити
11. Віруси – реплікатори так звані хробаки, що поширюються комп’ютерними мережами
12. Віруси невидимки – стелсвіруси які перехоплюють обертання ОС до уражених файлів і секторів дисків та підставляють замість свого тіла незаражені ділянки диска
13. Віруси мутанти які містять алгоритм шифрування – розшифрування
14. Квазивірусні, або «троянські програми» які неспроможні до само розповсюдження, проте дуже небезпечні, оскільки, маскируючись під корисну програму, руйнують завантажувальний сектор і файлову систему дисків

Антивірусні програми – програми для виявлення, видалення і захищення від комп’ютерних вірусів. Зазначені нижче варіанти програм сьогодні в чистому вигляді практично не зустрічаються. Розроблювачі антивірусів змушені передбачати практично всі основні типи антивірусних програм, які стосовно нинішніх питань безпеки правильно було казати компонентами або складовими, ніж самостійними додатками.

Програми – детектори або сканери основний елемент будь – якого антивірусу здійснює пасивний захист. За запитом користувача або заданим розпорядком провадить перевірку файлів у вибраній ділянці системи. Шкідливі об’єкти виявляє шляхом пошуку й порівняння програмного коду вірусу. Приклади програмних кодів міститься в здалегіть установлених сигнатурах (наборах, характерних послідовностей байтів для відомих вірусів). Серед недоліків цих програм – беззахисність перед вірусами, що не мають постійного програмного коду і здатні видозмінюватися зі збереженням основних функцій. Також сканери не можуть протидіяти різновидам того самого вірусу, що вимагає від користувача постійного оновлення антивірусних баз. Та найбільш уразливе місце – нездатність виявити нові й невідомі віруси.

Програми – монітори у сукупності зі сканером створюють базовий захист комп’ютера. На основі наявних сигнатур здійснює перевірку поточних процесів у режимі реального часу. Виконують попередню перевірку при спробі перегляду чи запуску файла. Розрізняють файлові монітори, монітори для поштових клієнтів, що використовують протоколи РОР3, ІМАР, NNTP і SMTP, і спеціальні монітори для окремих додатків. Основна їхня перевага – здатність виявляти віруси безпосередньо на ранній стадії активності.

Програми – лікарі або фаги знаходять зараженими вірусами файли та «лікують» їх, тобто видаляють із файла тіло програми віруса, повертаючи файли до вихідного стану. Спочатку фаги знаходять і знищують віруси в оперативній пам’яті, і тільки потім переходять до «лікування» файлів. Серед фагів виділяють поліфаги, програми – лікарі, призначені для пошуку і знищення великої кількості вірусів. З огляду на те, що постійно з’являються нові віруси, програми – детектори і програми – доктори швидко застарівають, і потрібно регулярне відновлення їх версій.

Програми – ревізори зберігають в окремій базі дані про стан критичних на певний момент для роботи ділянок системи. Згодом порівнюють поточні файли із зареєстровані раніше, в такий спосіб виявляючи будь – які підозрілі зміни. Перевага – низькі апаратні вимоги і висока швидкість роботи. Ревізорові взагалі непотрібна антивірусна база, сприйняття і знаходження відбуваються тільки на рівні незмінності вихідних файлів. Це дозволяє ефективно відновлювати систему, пошкоджену діяльністю шкідливих модулів. Недолік полягає в неможливості оперативного реагування на появу вірусу в системі. Під час перевірки також виключаються нові файли, що дозволяє вірусам, які заражають тільки заново створювані файли, залишитися.

Програми – фільтри або «сторожі» являють собою невеличкі резидентні програми, призначені для виявлення підозрілих дії при роботі комп’ютера, характерних для віруса (а саме : спроба корекції файлів із розширенням СОМ і ЕХЕ ; завантаження резидентної програми ). При спробі програми зробити зазначені дії «сторож» посилає користувачу повідомлення і пропонує зробити або дозволити відповідну дії. Програми – фільтри дуже корисні, оскільки здатні виявляти вірус на початковій стадії існування його до розмноження. Проте вони не «лікують» файли і диски, для знищення вірусів потрібно застосувати інші програми, наприклад фаги.

Програми – вакцини або імунізатори імітують зараження файлів певним вірусами, внаслідок чого справжні віруси зіштовхуються зі своїми «побратимами» і припиняють спроби зараження. Сьогодні цей тип програм практично не використовуються.

Спроби протидії комп’ютерними вірусами

* Профілактика вірусного зараження й зменшення передбачуваної шкоди від такого зараження.
* Методика використання антивірусних програм, у тому числі знешкодження й видалення відомого вірусу.

Способи виявлення й видалення невідомого вірусу

Способи захисту комп’ютера від зараження вірусами, а отже й забезпечити надійне зберігання інформації на дисках:

* Установити на комп’ютері сучасні антивірусні програми й постійно оновлювати їх версії
* Перед зчитування з дискет інформації, записаної на інших комп’ютерах, завжди перевіряти ці дискети на наявність вірусів ; перенесення на свій комп’ютер файли в архівіруваному вигляді перевіряти відразу після розархівування на жорстокому диску, обмежуючи ділянку перевірки тільки щойно записаними файлами ; періодично перевіряти на наявність вірусів жорсткі диски комп’ютера, запускаючи антивірусні програми для тестування файлів, пам’яті й системних ділянок
* Завжди захищати свої дискети від запису під час роботи на інших комп’ютерах, якщо на них не буде провадитися запис інформації
* Дистрибутивні копії програмного забезпечення необхідно купувати в офіційних продавців
* Періодично зберігати на зовнішньому носії файли, з якими ведеться робота