Інформатика

Комп'ютерний віруси

Виконав учень 9-А класу

Бондарев Андрій

Комп'ютерний вірус

- ***Комп'ютерний вірус*** *(англ. computer virus)* — комп'ютерна програма, яка має здатність до прихованого саморозмноження. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макро-віруси. Можливі також комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу. Необізнані користувачі ПК помилково відносять до комп'ютерних вірусів також інші види зловмисного ПЗ — програм-шпигунів чи навіть спам. За створення та поширення шкідливих програм (в тому числі вірусів) у багатьох країнах передбачена кримінальна відповідальність. Зокрема, в Україні поширення комп'ютерних вірусів переслідується і карається відповідно до Кримінального кодексу (статті 361, 362, 363). Приклади вірусів: Neshta, Staog,Archiveus.

Класифікація

- Не існує єдиної системи класифікації та іменування вірусів (хоча спроба створити стандарт була зроблена на зустрічі CARO в 1991 році).
- Прийнято розділяти віруси за:
- об'єктами, які вражаються (файлові віруси, завантажувальні віруси, анти-антивірусні віруси, скриптові віруси, макро-віруси, мережеві черв'яки).
- способом зараження (перезаписуючі віруси, віруси-компаньйони, файлові хробаки, віруси-ланки, паразитичні віруси, віруси, що вражають вихідний код программ)
- операційними системами і платформами, які вражаються (DOS, Microsoft Windows, Unix, Linux, інші)
- активністю (резидентні віруси, нерезидентні віруси)
- технологіями, які використовуються вірусом (нешифровані/шифровані віруси, поліморфні віруси, стелс-віруси (руткіт і буткіт))
- деструктивними можливостями (нешкідливі віруси, безпечні віруси, небезпечні віруси, дуже небезпечні віруси)
- мовою, якою написаний вірус (асемблер, високорівнева мова програмування, скриптова мова, інші).

Ознаки зараження вірусом

- Зменшення вільної пам'яті
- Уповільнення роботи комп'ютера
- Затримки при виконанні програм
- Незрозумілі зміни в файлах
- Зміна дати модифікації файлів без причини
- Незрозумілі помилки Write-protection
- Помилки при інсталяції і запуску ОС
- Відключення 32-розрядного допуску до диску
- Неспроможність зберігати документи Word в інші каталоги, крім Template
- Погана робота дисків
- Файли невідомого походження
- Ранні ознаки зараження дуже тяжко виявити, але коли вірус переходить в активну фазу, тоді легко помітити такі зміни:
- Зникнення файлів
- Форматування HDD
- Неспроможність завантажити комп'ютер
- Неспроможність завантажити файли
- Незрозумілі системні повідомлення, звукові ефекти і т. д.
- Здебільшого, все це в минулому. Зараз основні ознаки — самовільне відкривання браузером деяких сайтів (рекламного характеру), підозріло підвищений інтернет-трафік та повідомлення від друзів, що ваші листи електронної пошти до них містили вірус.

Види

Класичні віруси

Типи комп'ютерних вірусів різняться між собою за такими основним ознаками:

середовище проживання;

спосіб зараження.

Під «середовищем проживання» розуміються системні області комп'ютера, операційні системи чи докладання, в компоненти (файли) яких впроваджується код вірусу. Під «способом зараження» розуміються різні методи впровадження вірусного коду в заражаемые об'єкти.

Середовище проживання

По середовища проживання віруси можна розділити на:

файлові;

завантажувальні;

макро;

скриптовые.

Класичні віруси

- **Файловые віруси при своєму розмноженні тим чи іншим способом використовують файлову систему будь-якої (чи якихось) ОС. Вони:**
- **у різний спосіб впроваджуються у виконувані файли (найпоширеніший тип вірусів);**
- **створюють файлы-двойники (компаньон-вирусы);**
- **будують копії у різних каталогах;**
- **використовують особливості організації файлової системи (link-вирусы).**
- **Загрузочные віруси записують себе або у завантажувальний сектор диска (boot-сектор), або у сектор, у якому системний завантажник вінчестера (Master Boot Record), або змінюють покажчик на активний boot-сектор. Цей тип вірусів виявився досить распространён у 90-х, але зник із переходом 32-битные операційні системи та відмовою від використання дискет як основного способу обміну інформацією між. Теоретично можливо поява завантажувальних вірусів, заражающих CD-дискиі USB-флешек, але цей момент такі віруси не виявлено.**
- **Багато табличні і графічні редактори, системи проектування, текстові процесори мають макро-языки для автоматизації виконання повторюваних дій. Ці макро-языки мають складну структуру і найрозвиненіший набір команд. Макро-вирусы є програмами на макро-языках, вмонтованих у такі обробки даних. Для свого розмноження віруси цього використовують можливості макро-языков та їх допомоги переносять себе вже з зараженого файла (документа чи таблиці) до інших.**
- **Спосіб зараження**
- **Файловые віруси**
- **По способу зараження файлів віруси діляться на:**
- **перезаписывающие (overwriting);**
- **паразитичні (parasitic);**
- **вирусы-компаньоны (companion);**
- **вирусы-ссылки**

Загрузочні віруси

- Відомі цей час завантажувальні віруси заражають завантажувальний (boot) сектор гнучкого диска і boot-секторчи Master Boot Record (MBR) вінчестера. Принцип дії завантажувальних вірусів грунтується на алгоритми запуску ОС включення чи перезавантаженні комп'ютера - після необхідних тестів встановленого обладнання (пам'яті, дисків тощо.) програма системної завантаження зчитує перший фізичний сектор завантажувального диска (A:, 3: чи CD-ROM залежно від параметрів, встановлених в BIOS Setup) і передає нею управління.

Троянські програми

- Троянские програми різняться між собою за тими діям, що вони виробляють на зараженому комп'ютері.
- Backdoor - троянські утиліти віддаленого адміністрування
- Троянские програми цього є утилітами віддаленого адміністрування комп'ютерів у мережі. По функціональності вони в що свідчить нагадують різні системи адміністрування, розроблювані і поширювані фірмами-виробниками програмних продуктів.

Мережні хробаки

- Основним ознакою, яким типи хробаків різняться між собою, є спосіб поширення хробака - як саме він передає свою копію на віддалені комп'ютери. Іншими ознаками відмінності КЧ між собою є способи запуску копії хробака на заражаемом комп'ютері, методи запровадження у систему, і навіть поліморфізм, «стелс» й інші характеристики, властиві та інших типам шкідливого програмного забезпечення (вірусам і троянським програмам).