Презентація на тему: Комп’ютерні віруси

- Бащенко Андрій 9-Б клас

Що таке комп’ютерний вірус ?

Комп'ютерний вірус - спеціально створена невелика програма, здатна до саморозмноження, засміченню комп'ютера і виконанню інших небажаних дій.

ІСТОРІЯ КОМП'ЮТЕРНИХ ВІРУСІВ

Перша «епідемія» комп'ютерного вірусу сталася в 1986 році, коли вірус на ім'я Brain (англ. «Мозок») «заражав» дискети персональних комп'ютерів. В даний час відомо кілька десятків тисяч вірусів, що заражають комп'ютери і розповсюджуються по комп'ютерних мережах.

Як вони розповсюджуються ?

- Глобальна мережа Internet
- Електронна пошта
- Локальна мережа
- Комп'ютери «Загального призначення»
- Піратське програмне забезпечення
- Ремонтні служби
- Змінні накопичувачі

Як вони діють ?

- Загальне уповільнення роботи комп'ютера і зменшення розміру вільної оперативної пам'яті;
- Деякі програми перестають працювати або з'являються різні помилки в програмах;
- На екран виводяться сторонні символи і повідомлення, з'являються різні звукові та відеоефекти;
- Розмір деяких здійснимих файлів і час їх створення змінюються;
- Деякі файли і диски виявляються зіпсованими;
- Комп'ютер перестає завантажуватися з жорсткого диска

Як запобігти зараженню ?

- Захист локальних мереж
- Використання дистрибутивного ПО
- Резервне копіювання інформації
- Використання антивірусних програм
- Не запускати неперевірені файли

Комп'ютерні віруси можуть існувати в системі в різних стадіях функціонування

- 1. Латентна стадія. На цій стадії код вірусу знаходиться в системі, але ніяких дій не робить. Для користувача не помітний. Може бути обчислений скануванням файлової системи і самих файлів.
- 2. Інкубаційна стадія. На цій стадії код вірусу активується і починає створювати свої копії, поширюючи їх по пристроях зберігання даних комп'ютера, локальних і глобальних комп'ютерних мережах, розсилаючи у вигляді поштових повідомлень і так далі. Для користувача може бути помітний, оскільки починає споживати системні ресурси і канали передачі даних, в результаті чого комп'ютер може працювати повільніше, завантаження інформації з Інтернет, пошти та інших даних може сповільняться.
- 3. Активна стадія. На цій стадії вірус, продовжуючи розмножувати свій код доступними йому способами, починає деструктивні дії на які орієнтований. Помітний користувачеві, так як починає проявлятися основна функція вірусу - пропадають файли, відключаються служби, порушується функціонування мережі, відбувається псування обладнання.

Як їх позбутися ?

Для ефективної боротьби з вірусами розробники антивірусних програм створюють так звані антивірусні бази – сукупність даних про відомі на певний момент часу і способи боротьби з ними. Існуючі антивірусні програми відомих фірм – це комплексні програми, що мають властивості всіх перерахованих типів програм.

Антивіруси

- Антивірусні програми Антивірусні програми призначені для запобігання зараження комп'ютера вірусом і ліквідації наслідків зараження. У залежності від призначення і принципу дії розрізняють наступні антивірусні програми:
  сторожа або детектори - призначені для виявлення файлів заражених відомими вірусами, або ознак вказують на можливість зараження.
  Доктора - призначені для виявлення й усунення відомих їм вірусів, видаляючи їх з тіла програми і повертаючи її в початковий стан. Найбільш відомими представниками є Dr.Web, AidsTest, Norton Anti Virus.
  Ревізори - вони контролюють вразливі і тому найбільш атакуються компоненти комп'ютера, запам'ятовують стан службових областей і файлів, а в разі виявлення змін повідомляють користувачеві.
  Резидентні монітори або фільтри - постійно знаходяться в пам'яті комп'ютера для виявлення спроб виконати несанкціоновані дії.У разі виявлення підозрілого дії виводять запит користувачеві на підтвердження операцій.
  Вакцини - імітують зараження файлів вірусами. Вірус буде сприймати їх зараженими і не буде внедряться.Чаще всього використовуються Aidstest Лозинського, Drweb, Dr.Solomon

ПАМ'ЯТКА
Безпеки для користувача Домашнього комп'ютера

- Обмежити фізичний доступ до комп'ютера, встановити пароль на вхід в систему і відключати доступ в Інтернет, коли він не потрібний;
- Підписатися на інформаційні бюлетені Microsoft і регулярно оновлювати операційну систему;
- Відключити всі невикористовувані служби і закрити порти, через які можуть здійснюватися атаки;
- Ретельно налаштувати всі програми, що працюють з Інтернет, починаючи з браузера - наприклад, заборонити використання Java і ActiveX;
- Встановити і оновлювати антивірусну програму;

ПАМ'ЯТКА
Безпеки для користувача Домашнього комп'ютера

- Використовувати брандмауер, хоча б вбудований в систему, і уважно аналізувати його повідомлення і логи;
- Вкрай акуратно працювати з поштою, а також програмами для обміну повідомленнями та роботи з файлообмінними мережами, наприклад, слід відключити використання HTML в прийнятих листах;
- Ніколи не запускати програми сумнівного походження, навіть отримані з заслуговують довіри джерел, наприклад, з надісланого іншому письма;
- Ні за яких умов не передавати по телефону або поштою свої персональні дані, особливо паролі;
- Регулярно створювати резервні копії критичних даних.

ДЯКУЮ ЗА ПЕРГЛЯД !!!