Оленченко Ілля Кіт - 211

**Лабораторна робота №1.**

**Тема:** ”Комп’ютерні віруси: знайомство з принципами роботи. Захист від вірусів. Огляд основних антивірусних програм”

**Мета роботи:** ознайомитись з основними видами комп’ютерних вірусів, принципами їх роботи поширення і знищення. Розглянути програми для захисту від вірусів, принцип дії, ефективність, можливості.

**Теоретичні відомості**

**1.Комп'ютерні віруси, їх властивості і класифікація**

**1.1 Властивості комп'ютерних вірусів**

Зараз застосовуються персональні комп'ютери, в яких користувач має вільний доступ до всіх ресурсів машини. Саме це відкрило можливість для небезпеки, яка отримала назву комп'ютерного вірусу.

Що таке комп'ютерний вірус? Формальне визначення цього поняття до цих пір не придумане, і є серйозні сумніви, що його взагалі може бути дано. Численні спроби дати «сучасне» визначення вірусу не привели до успіху. Тому ми обмежимося розглядом деяких властивостей комп'ютерних вірусів, які дозволяють говорити про них як про деякий певний клас програм.

Перш за все, вірус - це програма. Таке просте твердження саме по собі здатне розвіяти безліч легенд про незвичайні можливості комп'ютерних вірусів. Вірус може перевернути зображення на вашому моніторі, але не може перевернути сам монітор. До легенд про віруси-вбивці, «що знищують операторів за допомогою виведення на екран смертельної колірної гамми 25-м кадром» також не варто відноситися серйозно. На жаль, деякі авторитетні видання час від часу публікують «найсвіжіші новини з комп'ютерних фронтів», які при найближчому розгляді виявляються наслідком не цілком ясного розуміння предмету.

Вірус - програма, що володіє здібністю до самовідтворення. Така здатність є єдиним засобом, властивим всім типам вірусів. Але не тільки віруси здібні до самовідтворення. Будь-яка операційна система і ще безліч програм здатні створювати власні копії. Копії ж вірусу не тільки не зобов'язані повністю співпадати з оригіналом, але, і можуть взагалі з ним не співпадати! Вірус не може існувати в «цілковитій ізоляції»: сьогодні не можна уявити собі вірус, який не використовує код інших програм, інформацію про файлову структуру або навіть просто імена інших програм. Причина зрозуміла: вірус повинен яким-небудь способом забезпечити передачу собі управління.

**2. Хід роботі**

**2.1. Принцип роботи вірусу Хробак(вірус-реплікатор)**

Хробак (мережний хробак) — тип шкідливих програм, що поширюються по мережних каналах, здатних до автономного подолання систем захисту автоматизованих і комп’ютерних мереж, а також до створення й подальшого поширення своїх копій, що не завжди збігаються з оригіналом, і здійсненню іншого шкідливого впливу.

* 1. **Приклади вірусів типу Хробак.**

**1) Хробак Морріса**

Зразок експерименту, над яким втратили контроль, і це привело до незапланованих наслідків. У листопаді 1988 року Роберт Морріс  вирішив дослідити розміри існуючої на той час комп’ютерної мережі і використав для цього вірус, додавши в нього функцію самокопіювання. Хробак вийшов з-під контролю і спровокував епідемію, заразивши більше 6 000 ПК мережі ARPANET. Збитки від вірусної атаки склали 96,5 мільйонів доларів.

**2) Хробак Heartbleed**

Шкідлива програма, яка навесні 2014 року змусила хвилюватися весь віртуальний світ. Вірус, випадково створений програмістом Робіном Сеггельменом, використав уразливості криптографічного пакету  OpenSSL і проник за короткий термін майже на півмільйона інтернет-сайтів. Heartbleed вкрав особисті дані, інформацію про кредитні карти, паролі у багатомільйонної аудиторії користувачів мережі.

**3) Хробак Sasser**

Творіння 17-річного школяра з Німеччини розпочало своє поширення мережею навесні 2004 року. Під прицілом вірусної атаки опинилися досить серйозні цілі: Британська берегова охорона, авіакомпанія Delta Airlines, інформаційна агенція France-Presse, десятки комп’ютерних мереж великих корпорацій, університетів, лікарень. Збиток від цього вірусу нараховує сотні мільярдів доларів. Але винуватець цих подій, будучи неповнолітнім, так і залишився непокараним.

**4) Вірус WIN.CIH (Чорнобиль)**

26 квітня 1999 року на тисячах ПК по всьому світу активізувався вірус, подібних якому ще не було. Використовуючи уразливості ОС Windows 95/98 , він через електронну пошту поширювався від комп’ютера до комп’ютера і пошкоджував вміст жорстких дисків, а подекуди і мікросхеми BIOS. Від вірусу  WIN.CIH (Чорнобиль) постраждало 300-500 тисяч ПК, розмір збитків сягає 80 мільйонів доларів.

Автором “Чорнобиля” виявився студент з Тайваню, який розповсюдив вірус в мережі за рік до активації. Це було перше шкідливе ПЗ, яке інфікувало не лише приватні машини, але й веб-сайти. Прописавшися на ігрових серверах, вірус зміг поширитися у Сполучених Штатах. Але найбільш постраждалим регіоном виявилася Східна Азія.

**5) Melissa**

В березні 1999 року віртуальний світ вразила епідемія вірусу Melissa, який відносять до категорії мережевих хробаків. Його творець Девід Сміт попередньо розмістив файли з вірусом на деяких форумах у вигляді списку з переліком сайтів для дорослих і паролями доступу до них. Протягом двох днів, використовуючи поштовий сервіс Microsoft Outlook, Melissa поширила свої копії на сотні тисяч ПК. Через вірусну атаку тимчасово були вимушені відключити свої e-mail сервери такі гіганти, як  Intel та Microsoft, щоб попередити подальше розповсюдження шкідливої програми. З кожного зараженого комп’ютера вірус розсилав свої копії у вигляді спаму на 50 перших адрес із списку контактів користувача. Таким чином було інфіковано близько мільйона ПК і нанесено збитків на 80 млн. доларів.

**2.3 Життєвий цикл вірусу**

Так само як для вірусів, життєвий цикл хробаків можна розділити на певні стадії:

1. Проникнення в систему
2. Активація
3. Пошук “жертв”
4. Підготовка копій
5. Поширення копій

Стадії 1 й 5, загалом кажучи, симетричні й характеризуються в першу чергу використовуваними протоколами й додатками.

Стадія 4 – Підготовка копій – практично нічим не відрізняється від аналогічної стадії в процесі розмноження вірусів.

**2.4 Методи поширення вірусу**

Найбільше часто серед хробаків зустрічаються спрощені реалізації метаморфізму. Деякі хробаки здатні розсилати свої копії в листах, як із впровадженням скріпта хробака, що приводить до автоматичної активації, так і без впровадження. Таке поводження хробака обумовлене двома факторами: скріпт автоматичної активації підвищує ймовірність запуску хробака на комп’ютері користувача, але при цьому зменшує ймовірність проскочити антивірусні фільтри на поштових серверах.

Аналогічно, хробаки можуть міняти тему й текст інфікованого повідомлення, ім’я, розширення й навіть формат вкладеного файлу – виконує модуль, що, може бути прикладений як є або в заархівованому виді.

**2.5 Програми для знищення вірусу Хробак**

* *Kaspersky Rescue Disk* - програма, що дозволяє очистити жорсткі диски від вірусів шляхом управління системою. Щоб почати роботу з програмою, потрібно записати завантажувальний диск через ISO-образ. А після просто запустити операційну систему в BIOS через нього.
* *Kaspersky Virus Removal Tool* більше підійде для початківців користувачів і тих, хто ще не розібрався в тонкощах системи. Він здійснює пошук шкідливих програм на комп'ютері і видаляє їх з системи. Однак впоратися він може не з усіма видами вірусів.
* *Dr.Web CureIt* цілком може замінити попередню антивірусну програму. Його величезний мінус в тому, що сканування жорстких дисків здійснюється дуже довго. Часом це може зайняти близько десяти годин. Звичайно, така довга перевірка є знаком того, що програма ретельно сканує кожен файл. Однак знайдеться небагато бажаючих витратити весь день на пошук одного вірусу.

**2.6 Методи знищення вірусу**

Для знищення комп’ютерних вірусів на вашому комп’ютері існує два основних методи.

    Перший полягає в повному форматуванні  жорсткого диску та переустановленні операційної системи разом з прикладним програмним забезпеченням . Не треба забувати також про вилучення всієї інформації з електронних поштових скриньок. Цей метод можна використати, якщо на жорсткому диску немає ніяких цінних даних, або якщо для цінних даних  зроблені резервні копії (перед форматуванням жорсткого димка треба пересвідчитись, що резервні копії дійсно існують і не втрачені з якихось причин). Метод повного форматування жорсткого диска вимагає багато часу на його реалізацію, але дає стовідсоткову гарантію видалення комп’ютерних вірусів.

    Другий метод знищення комп’ютерних  вірусів полягає у використанні  спеціальних антивірусних програм.  Цей метод не дає стовідсоткової гарантій видалення вірусів. До того ж відомі ситуації, коли при спробі використання антивірусних програм руйнувалися дані, якими ще можна було користуватись і які ще можна було врятувати.

Звичайно  антивірусні програми мають у  своєму складі:

* програму-сканер для перевірки дисків, знищення вірусів та лікування заражених програм і даних;
* програму-охоронця, яка автоматично завантажується в оперативну пам'ять після включення комп’ютера та виконує перевірку на віруси всіх файлів, з якими відбувається робота; також програма-охоронець звичайно відстежує всі звернення до жорсткого диска (бо руйнівні дії вірусів так чи інакше призводять до модифікації даних, які зберігаються на жорсткому диску комп’ютера);

**Висновки**

На цій лабораторній роботі я ознайомився з основними видами комп’ютерних вірусів, принципами їх роботи поширення і знищення. Розглянув програми для захисту від вірусів, принципи їх дій, ефективності та можливості.