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.

1.2. Класифікація вірусів

На сьогодні відомі десятки тисяч вірусів, які в цілому мають конкретну класифікацію. Спробуємо детальніше розглянути основні групи, на які поділяються комп'ютерні віруси.

I. Поділ вірусів за середовищем їх розповсюдження:

- Завантажувальні віруси - це найбільш небезпечна група вірусів, що заражають Boot Record та Master Boot Record логічних та фізичних дисків. Про ці віруси ми вже говорили попередньо.
- Файлові віруси. Ці віруси поширюються, заражаючи файли різних типів, як вже було сказано, - найчастіше це виконуючі файли та файли оверлеїв. До цієї групи слід також віднести макровіруси, хоч інколи їх виділяють як окремий клас вірусів.
- Завантажувально-файлові віруси здатні вразити як код завантажувальних секторів, так і код файлів, як правило системних.
- Віруси сімейства Dir використовують інформацію про файлову структуру та вміст каталогів (див. попередній матеріал).
- Multipartition - віруси можуть вражати одночасно виконуючі файли, boot - сектор, MBR, FAT і каталоги і є найбільш небезпечними, особливо, якщо вони ще й володіють поліаморфними властивостями і елементами невидимості.
- Мережеві віруси - це віруси, що поширюються як сукупність машинного коду в комп'ютерних мережах.
- Поштові віруси - на сьогодні досить нова але надзвичайно поширена група вірусів, що розповсюджуються разом із поштовими повідовленнями у вигляді прикріплених до них файлів (Attachment) із програмним кодом. Як правило, такі віруси досить швидко розмножуються і час від часу викликають вірусні епідемії (згадати, хоча б, такі резонансні в останні роки віруси як "I Love You" (LoveLetter), Melissa або "Anna Kournicova").

II. Класифікація комп'ютерних вірусів за алгоритмом роботи:

- Віруси "паразити" найпростіші віруси що використовують "тіло" інших файлів (виконуючих), записуючи туди себе. Вони можуть бути досить легко виявлені і знешкоджені.
- Віруси супутники створюють копію exe-файлу з розширенням com і записують туди себе. Коли з командного рядка DOS завантажують такий файл, то як правило розширення не вказують, а за правилами DOS, першим завантажується com файл, тобто вірус.
- Віруси "черв'яки" (віруси-реплікатори) не створюють собі файлу, а поширюються лише в комп'ютерних мережах та в оперативній пам'яті у вигляді певного машинного коду. Вони ніби черв'яки проникають в оперативну пам'ять ПК через комп'ютерну мережу, пронизуючи системи захисту. Найбільш грізними представниками цього типу вірусів є Nimda (неодноразовий переможець рейтингів найнебезпечніших вірусів), Gigger та Redesi (здатні відформатувати диск C), Bumerang (здатний знищити FlashBIOS та таблиці файлової системи вінчестера), SirCam (найдзвичано швидкий у розповсюдженні та знищує інформацію на диску C), Кігау та Paukor (знищують всі файли із системних папок Windows).
- Студентські віруси - це віруси, які мають в собі багато помилок і написані, як правило, початківцями.
- Віруси "невидимки" (Stealth - віруси) фальсифікують інформацію, перехоплюючи звертання антивірусної програми, до заражених ділянок диску і

направляючи її на незаражені. Вірус перехоплює вектор переривання int 13h. Ця технологія використовується, як у файлових, так і в завантажувальних вірусах.

- Віруси "мутанти" ("привиди") або поліаморфні (polimorphic) - не мають постійної сигнатури (машинного коду), за якою можна було б виявити вірус. Вони міняють сигнатуру з кожною копією і тому з ними важко боротись. Виявляють такі віруси лише за допомогою еврістичного аналізу, коли антивірусна програма "прокручує" алгоритм роботи виконуючих файлів і в разі підозрілих операцій приймає це за вірус. Таким же чином антивірусні програми шукають невідомі ще їм віруси.
- Ретровіруси - це звичайні файлові віруси, які прагнуть заразити антивірусні програми, знищуючи їх або роблячи непрацездатними. Тому практично всі антивіруси в першу чергу перевіряють свої власні розміри і контрольну суму.
- "Троянські" віруси (Trojans) здійснюють шкідливі дії замість оголошених легальних функцій або разом з ними. Вони переважно не здатні на саморозповсюдження і передаються тільки при копіюванні користувачем. Часто ці віруси використовують в якості "шпигунів". Проникаючи по мережі на ПК, вони стараються "затаїтись" і "вкрасти" паролі користувача (особливо виходу в Internet) і передати їх господарю. Деякі троянські віруси готують грунт на зараженому ними ПК для проникнення без перешкод інших вірусів, що слідують за ними. Боротись з такими вірусами (особливо новими) досить важко, адже в їх коді немає ніякої дистуктивної дії (не міняється розмір інших файлів, не форматуються диски), а навпаки вони стараються ніяк себе не проявити. Для боротьби з такими вірусами використовуються спеціальні програми FireWoll (файрволл) - мережеві екрани, які під час підключення до мережі слідкують чи не пробує якась програма на ПК вийти в Internet. Якщо така спроба відбулась, то вона блокується і виводиться повідомлення, із запитом дозволу на таку операцію. Корисною функцією файрволл є те, що він може захистити не лише від троянських вірусів, але й від хакерських атак із зовні (з Internet). Потрібно відмітити, що існує багато відомих троянських вірусів, які не лише виступають в ролі "шпигунів" але й самі несуть досить високу деструктивну дію (наприклад TROJ_ZERAF знищує EXE і SYS файли та робить помилки в системному реєстрі).
- Віруси таймери очікують лише певного часу (певної години, дня і т.д.), і лише тоді спрацьовують.

III. Поділ вірусів за деструктивною дією:

- Нешкідливі віруси - це віруси, які не приносять жодної шкоди, а просто себе копіюють багато разів, заповнюючи диски, або загромаджуючи оперативну пам'ять.
- Не небезпечні віруси схожі до попередніх, але крім цього їх дія супроводжується різними спецефектами (відеота звуковими).
- Небезпечні віруси - це віруси дія яких призводить до серйозних збоїв в роботі ПК, таких як зависання комп'ютера іт.д.
- Дуже небезпечні віруси - це віруси, дія яких супроводжується знищенням інформації (файлів, каталогів, форматування цілих дисків). В січні

1998 року, завдяки журналу "Virus Bulletin", з'явився термін WildList (список "диких вірусів"). Він регулярно поновлюється і публікується цим авторитетним міжнародним виданням.

IV. Класифікація вірусів за принципом дії:

- Резидентні - це віруси, що завантажуються в оперативну пам'ять і постійно там знаходяться, аж до виключення живлення чи перезавантаження ПК.
- Нерезидентні - це віруси, які короткочасно завантажуються в пам'ять, виконують потрібні їм дії і вивантажуються з пам'яті.

V. Поділ вірусів за місцем втілення у файли:

- **На початку файлу.**
- **Всередині файлу.**
- **В кінці файлу.**

2. Види файлів, які можуть бути заражені вірусом.

Як правило, кожна конкретна різновидність вірусу може заразити тільки один або два типи файлів. На даний час частіше всього зустрічаються макровіруси, тоді як в 90-ті роки найпоширенішими були віруси, що заражали COM-файли, а на другому місці - EXE-файли.

Види файлів, які можуть бути заражені вірусом:

- **виконуючі файли**, тобто файли з розширеним ім'ям COM і EXE, а також оверлейні файли, завантажені іншими програмами. Вірус в заражених виконуючих файлах починає свою роботу при завантаженні тієї програми, в якій він знаходиться;
- **файли документів та шаблонів**, створених програмами Word, Excel, Access та іншими офісними програмами, а точніше макроси, що використовуються там. Цей тип вірусів порівняно молодий і називають його макровірусами. Деякі з вірусів цього типу є надзвичайно шкідливими. Наприклад вірус W97M.Thus при активізації 13 грудня здатний знищити всі файли на диску C, зберігаючи при цьому структуру каталогів (папок).
- **блок початкового завантаження** операційної системи і головний завантажувальний запис жорсткого диску. Вірус, який заразив ці ділянки, як правило, складається з 2-х частин, оскільки на цих ділянках диску, важко розмістити програму вірусу в цілому. Частина вірусу, що не поміщається в них, розташована на іншій ділянці диску, який оголошується дефектним. Такий вірус починає свою роботу при початковому завантажуванні операційної системи і є резидентним, тобто постійно знаходиться в пам'яті комп'ютера. Відомі випадки, коли вірус форматує додаткову доріжку диску, куди і записує основну частину програми;
- **таблиці файлової системи та каталоги**. Як відомо, в кожен каталог записуються імена файлів, дата та час створення, номер першого кластера файлу, а також резервні байти, що ОС не використовуються. Віруси цього типу, записавшись в кластери, помічають їх як пошкоджені, а тоді реорганізовують файлову систему. При цьому інформація про перші кластери деяких виконуючих файлів записується у резервні біти, а на її місце поміщається посилання на тіло вірусa. Тому, при спробі користувача завантажити відповідну програму - вірус

отримує керівництво. Цей тип вірусів, з'явившись в 1991 році, викликав в Росії справжню епідемію, яку можна порівняти із чумою.

- **драйвери пристроїв**, тобто файли, які здійснюють програмне керування зовнішнім пристроєм. Вірус, який знаходиться в цих файлах, починає свою роботу при кожному звертанні до відповідного пристрою;
- **системні файли**, тобто файли IO.SYS і MSDOS.SYS. Це досить небезпечно, оскільки вони, як і у випадку зараження блоків початкового завантаження дисків, починають діяти при кожному завантаженні ПК.

3. Шляхи проникнення вірусів в комп'ютер

Розглянемо, тепер, яким чином комп'ютерний вірус може потрапити на ПК звичайного користувача. На початку їх існування основним середовищем розповсюдження вірусів були переносні диски, переважно дискети. Пізніше, із набуттям популярності CD-дисків вони також стали зручним середовищем поширення вірусів (перш за все це не ліцензійні програмні продукти). В другій половині 2001 року комп'ютерні віруси проникли і на DVD (вірус Funvole).

В другій половині 90-х років основним середовищем розповсюдження комп'ютерних вірусів стали комп'ютерні мережі та електронна пошта. Це викликано надзвичайно бурхливим розвитком Internet, що дозволило фактично миттєво поширюватись новим вірусам на дуже великі території.

Прикладом може бути 2001 рік, визнаний відомими міжнародними антивірусними виданнями роком троянських вірусів та поштових черв'яків, а лідером серед вірусів став поштовий черв'як Nimda.

Варто пам'ятати проте, що розробники комп'ютерних вірусів не зупиняються на досягнутому і шукатимуть нові шляхи розповсюдження комп'ютерних вірусів. Так, наприклад, відомі вже випадки поширення вірусів через файли в форматі RTF, PDF та анімаційні файли, створені в Macromedia Flash (перший відомий вірус SWF/LFM-926).

4. Захист від комп’ютерних вірусів.

4.1. Класифікація антивірусних програм.

Комп'ютерний вірус - це дуже неприємне шкідливе явище, побачити яке на своєму ПК не хотів би, напевне, жоден користувач. Застрахуватись від вірусів на сьогодні повністю неможливо, хіба що зовсім ізолювати ПК від обміну інформацією із навколишнім світом. Але робити це, напевне ніхто не буде, адже тоді ПК втратить багато своїх переваг.

Необхідно застосовувати спеціалізовані програми для захисту від вірусів. Ці програми можна поділити на декілька видів.

- **детектори** - дозволяють знайти файли, заражені яким-небудь одним, наперед відомим нам вірусом, або одним з багатьох відомих вірусів;
- **вакцини** (іммунізатори) - модифікують (інфікують) програми і диски таким чином, що це не відображається на роботі програм. Після цього вірус, від якого виконується вакцинація, вважає ці програми або диски вже інфікованими і повторно їх не заражає;

- **лікарі** (фаги) - лікують заражені програми або диски "викусуючи" із заражених програм тіло віруса, тобто відновлюючи програму в тому стані, в якому вона була до зараження вірусом;
- **ревізори** - спочатку запам'ятовують стан інформації (розмір, дату і час створення) і системних ділянок дисків, а потім порівнюють його з поточним. При виявленні невідповідностей про це повідомляється користувачу;
- **лікарі-ревізори** - це гібриди ревізорів і лікарів, тобто програми, які не тільки помічають зміни в файлах і системних ділянках дисків, але й можуть у випадку виявлення змін вилікувати заражені файли;
- **фільтри** (монітори) - резидентні програми для захисту від вірусів, які поміщаються резидентно в оперативній пам'яті комп'ютера і перехоплюють звернення вірусів до системних ділянок і файлів. Користувач може дозволити або заборонити виконання відповідних операцій;
- **поліфаги** - це найбільш ефективніша група програм, що поєднують в собі декілька вище приведених типів антивірусів, наприклад, фільтрів, детекторів та лікарів.

4.2. Огляд антивірусних засобів.

Темі боротьби з комп'ютерними вірусами в світі приділяється багато уваги. Багато великих та малих компаній займаються розробкою нових та ефективних програм для захисту ПК від вірусів. Найбільш впливовим і авторитетним показником ефективності антивірусних програм є рейтинг, який щомісяця проводить міжнародний комп'ютерний журнал Virus Bulettin (Англія).

Проводяться тестування, при яких антивіруси встановлюються в однакових умовах на заражені різними типами вірусів комп'ютери і визначається відсоток виявлених та знешкоджених ними вірусів. Тестування проводиться по таких основних категоріях, як wild ("дикі"), макровіруси, поліморфні та стандартні. При тестуванні враховуються також такі параметри як швидкість роботи програми, її вартість та зручність інтерфейсу. Сама участь антивірусної програми в тестуванні вже є великим визнанням для неї.

Порядок виконання роботи

1. Ознайомитись з основними типами вірусів.
2. Вибрати один з типів вірусів:
    a. Розглянути принцип роботи даного типу вірусів;
    b. Навести назви вірусів даного типу;
    c. Методи поширення даного типу вірусів;
    d. Які існують програми для знищення даного типу вірусів;
    e. Які методи використовують для знищення даного типу вірусів.
3. Оформити звіт по роботі
    a. Звіт повинен включати:
        - тему, мету роботи;
        - короткий виклад основних теоретичних положень;

- тип, параметри досліджуваного у роботі класу вірусів;
- алгоритм роботи вірусу;
- методи знищення вірусу;
- висновки.

Контрольні запитання

1. Що таке комп’ютерний вірус?
2. Властивості вірусів?
3. Як працюють віруси?
4. Як розповсюджуються комп’ютерні віруси?
5. Поняття зараженої програми?
6. Які файли можуть бути заражені вірусом?
7. Що таке Інтернет – хробаки?
8. Які принципи роботи троянських програм?
9. Що таке антивіруси?
10. Як функціонують антивірусні програми?
11. Класи антивірусних програм.