Тема 9. Комп'ютерні віруси та методи боротьби з ними.

Мета: Ознайомити студентів з комп'ютерними вірусами, антивірусними програмами та основними методами боротьби.

1. Поняття та класифікація комп'ютерних вірусів
2. Захист від вірусів.

1. Поняття та класифікація комп'ютерних вірусів.

Комп'ютерним вірусом називається невелика програма (розміром не більш як 500 байт), що самостійно запускається, багаторазово копіює свій код і впроваджує його у файли, системні області дисків, обчислювальні мережі тощо. Створенні в такий спосіб копії вірусу зберігають здатність до подальшого самовідтворення в поширення. Об'єкти, у які впроваджуються комп'ютерні віруси, називаються середовищем існування вірусів.

Віруси можна розділити на класи по наступним основних ознаках:

- середовище існування;
- операційна система (ОС);
- особливості алгоритму роботи;
- деструктивні можливості.

По середовищу існування віруси можна розділити на:

- файлові;
- завантажувальні;
- макро;
- мережні.

Файлові віруси або різні способи впроваджуються у виконувані файли (найбільш розповсюджений тип вірусів), або створюють файли-двійники (компаньйони-віруси), або використовують особливості організації файлової системи (link-віруси).

Завантажувальні віруси записують себе або в завантажувальний сектор диска (boot-сектор), або в сектор, що містить системний завантажник вінчестера (Master Boot Record), або змінюють покажчик на активний boot-сектор.

Макро-віруси заражають файли-документи й електронні таблиці декількох популярних редакторів.

Мережні віруси використовують для свого поширення чи протоколи команди комп'ютерних мереж і електронної пошти.

Серед особливостей алгоритму роботи вірусів виділяються наступні пункти:

- резидентність;
- використання стелс-алгоритмів;
- самошифрування і поліморфічность;
- використання нестандартних прийомів.

Резидентний вірус при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, що потім перехоплює звертання операційної системи до об'єктів зараження і впроваджується в них. віруси знаходяться в пам'яті і є активними аж до вимикання чи комп'ютера перезавантаження операційної системи. Нерезидентні віруси не заражають пам'ять комп'ютера і зберігають активність обмежений час. Деякі віруси залишають в оперативній пам'яті невеликі резидентні програми, що не поширюють вірус. Такі віруси вважаються нерезидентними.

Резидентними можна вважати макро-віруси, оскільки вони постійно присутні в пам'яті комп'ютера на увесь час роботи зараженого редактора. При цьому роль операційної системи бере на себе редактор, а поняття «перезавантаження операційної системи» трактується як вихід з редактора.

Використання Стелс-алгоритмів дозволяє вірусам чи цілком частково сховати себе в системі. Найбільш розповсюдженим стелс-алгоритмом є перехоплення запитів ОС на читання/запис заражених об'єктів. Стелс-віруси при цьому або тимчасово лікують їх, або «підставляють» замість себе незаражені ділянки інформації. У випадку макро-вірусов найбільш популярний спосіб — заборона викликів меню перегляду макросів. Один з перших файлових стелс-вірусов — вірус «Frodo», перший завантажувальний стелс-вірус — «Brain».

Самошифрування і поліморфічність використовуються практично всіма типами вірусів для того, щоб максимально ускладнити процедуру виявлення вірусу. Полиморфик-віруси (polymorphic) - це досить важковиявлені віруси, що не мають сигнатур, тобто не утримуючі жодного постійної ділянки коду. У більшості випадків два зразки того самого поліморфік-віруса не будуть мати жодного збігу. Це досягається шифруванням основного тіла вірусу і модифікаціями програми-розшифровувача.

Різні нестандартні прийоми часто використовуються у вірусах для того, щоб якнайглибше сховати себе в ядрі ОС (як це робить вірус «ЗАРАЗА»), захистити від виявлення свою резидентну копію (віруси «TPVO», «Trout2»), утруднити лікування від вірусу (наприклад, помістивши свою копію в Flash-BIOS) і т.д.

По деструктивних можливостях віруси можна розділити на:

- нешкідливі, тобто ніяк що не впливають на роботу комп'ютера (крім зменшення вільної пам'яті на диску в результаті свого поширення);
- безпечні, вплив яких обмежується зменшенням вільної пам'яті на диску і графічними, звуковими й ін. ефектами;
- небезпечні віруси, що можуть привести до серйозних збоїв у роботі комп'ютера;
- дуже небезпечні, в алгоритм роботи яких свідомо закладені процедури, що можуть привести до втрати програм, знищити дані, стерти необхідну для роботи комп'ютера інформацію, записану в системних областях пам'яті, і навіть, як говорить одна з неперевірених комп'ютерних легенд, сприяти швидкому зносу частин механізмів, що рухаються - вводити в резонанс і руйнувати голівки деяких типів вінчестерів.

2. Захист від вірусів

Для виявлення та ліквідації вірусів розроблені сотні різних антивірусних програм. Однак ні одна антивірусна програма не може гарантувати 100 % виявлення і усунення вірусу. До того ж самі антивіруси! програми іноді с джерелами нового вірусу. Один вірус вони мажуть знищити, а інший, новіший,— внести.

Антивіруси можна поділити на спеціалізовані і універсальні.

Спеціалізовані антивірусні програми здатні знаходити та ліквідовувати тільки певні типи уже відомих вірусів. З невідомими вірусами ці програми боротися не можуть.

Щодо надійності виявлення вірусу спеціалізовані програми значно переважають універсальні.

Універсальні антивіруси, орієнтовані на цілі класи вірусів, в свою чергу, поділяються на резиденті і ревізори. Резиденті постійно присутні у внутрішній пам'яті комп'ютера і періодично здійснюють перевірку на наявність вірусів. Антивіруси-ревізори здатні лише встановити, чи піддавався файл будь-яким змінам (у тому числі і вірусним) після останнього його використання.

Найпопулярнішими серед користувачів є антивірусні програми Нортон Антивірус, AVP Касперського та інші.

Розглянемо найбільш поширені програми для боротьби з цим злом.

Aidstest є поліфагом. Це означає, що він може виявити і знищити відомий йому вірус. Aidstest приблизно розпізнає 5000 вірусів. Він не може також перевіряти запаковані файли і файли, захищені вакцинами і на кінець не володіє здатністю до евристичного аналізу, оскільки не може розпізнавати дію невідомого йому вірусу. Але все одно він залишається антивірусом з непоганою базою даних про звичайні, не поліморфні віруси; в особливості це торкається старих вірусів, яких родич Aidstesta, Dr Web, «за молодістю років» може просто не знати.

Dr Web - сильний антивірус з міцним алгоритмом виявлення вірусів. Так же, як і Aidstest, є поліфагом, однак на відміну від нього, може «читати» запаковані файли та архіви, файли даних в форматах WinWord і Excel, і знешкоджує поліморфні віруси, які в останній час отримують все більше поширення. Досить сказати, що епідемію дуже безпечного поліморфного вірусу OneHalf зупинив саме Dr Web. Евристичний аналізатор Dr Web, що досліджує програми в пошуках ділянок коду, характерних для вірусів, дозволяє виявити 90% невідомих вірусів. Цікаво, що різниця в кількості виявлення вірусів для слабкого і сильного евристичного аналізу при відключеному сигнатурному пошуку не така й велика - 81% і 90% відповідно (різниця в швидкості перевірки більш істотна.

При запуску програми першим ділом Dr Web перевіряє самого себе на цілісність, після чого тестує оперативну пам’ять - в залежності від установок, 640 КВ або 1 МВ (включає МНА). Рекомендується перевіряти всю пам’ять - в цьому випадку процес перевірки продовжується трохи довше, але справа в тому, що вже давно існують віруси, здатні загружатися в верхню пам’ять.

Алгоритм роботи цього антивірусу в тому, що він емулює процесор, тобто створює програмну модель комп'ютера, на якій проганяє дослідницькі програми і відсліджує всі операції, виконуємі ними в даній моделі.

ANTIVIRAL TOOLKIT PRO BY EUGENE KASPERSKY НТЦ КАМІ

Цей антивірус по відомості не на багато поступається комплекту від "ДіалогНаука". AVP є поліфагом і в процесі роботи перевіряє оперативну пам'ять (включаючи XMS і EMS), файли, в тому числі архівні і упаковані, а також системні сектори, які містять Master Boot Record, завантажувальний сектор (Boot-сектор) і Partition Table. На відміну від Dr Web і Aidstest, AVP розпізнає більше 100 тисяч вірусів, серед них поліморфні, stealh- і макровіруси, а також «троянські програми». Програма насичена евристичним сканером, котрий, по твердженню розробників антивірусу з КАМІ, виявляє близько 80% всіх вірусів. Можна встановити різні режими сканування - в стандартному режимі перевіряються тільки «крапки входу». тобто місця, в яких починається обробка програми системою, в той час як в режимі сканування відбувається повна обробка вмісту досліджувальних файлів. Правда, самі розробники рекомендують включати надлишкове сканування лише в тих випадках, коли стандартний режим не виявив вірус. Особливістю цього антивірусу є також його здатність до самолікування.

Нові антивіруси бази до AVP з'являються приблизно 1 раз на тиждень. В них включається інформація про всі віруси, які виникли за цей час, і розширений лікуючий модуль для цих вірусів. Данні бази розповсюджуються безкоштовно і доступно через Internet.

В теперішній час існують версії AVP для DOS, Windows 98/2000 , Novell, NetWare, також ведуться розробки для Windows NT Server і OS/2, для Macintosh.

NORTON ANTIVIRUS FOR WINDOWS

Серед українських користувачів антивірус Пітера Нортона є найбільш популярним з західних програм даного класу. І це не дивно, зважаючи на існування локалізованої версії антивірусу і просто міжнародну любов до програмних продуктів Пітера.

Norton AntiVirus визначає близько 10 тисяч вірусів, враховуючи поліморфні віруси і stealth. Пакет утримує сканер для сигнатурного пошуку є можливістю перевірки запакованих файлів, програму-сторож, контролюючі дії всіх програм при виконанні, створенні і відкритті файлів, а також при намаганні запису в MBR. Дуже великі можливості представляє антивірус при настройці особистих списків, перевіряємих файлів і перегляду журналу активності.

В комплект поставки Norton AntiVirus входить Norton Scheduler, котрий дозволяє створювати особисті графіки антивірусної перевірки, в тому числі і мережних дисків. Антивірус підтримує оновлення по Internet і невелику енциклопедію вірусів. Одною з зручних особливостей пакета є перевірка окремо взятої директорії і навіть файлу.

Питання для самоконтролю:

1. Що таке "комп'ютерний вірус" і яку шкоду він може завдавати?
2. Як можна класифікувати комп'ютерні віруси?
3. Як ведеться боротьба з вірусами?
4. Як запобігти зараженню комп'ютерним вірусом?
5. Як провести антивірусну обробку диска?

Увага ! *Матеріал даної теми обов'язково законспектувати і вивчити.*