ПОНЯТТЯ ПРО КОМП'ЮТЕРНІ ВІРУСИ

1. Означення комп'ютерного вірусу

- Комп'ютерний вірус це невелика програма, що написана програмістом високої кваліфікації, здатна до саморозмноження й виконання різних деструктивних дій.
- Комп'ютерний вірус – це програма, яка маскує своє перебування на комп'ютері, виконує небажані дії без відома користувача і має властивість розповсюджуватися без керування людиною.
- Комп'ютерним вірусом називають певну сукупність виконуваного машинного коду, яка може створювати свої копії (що не обов'язково співпадають з оригіналом) і вміщувати їх у файли, системні області комп'ютерів, комп'ютерні мережі. Вірус — це своєрідна програма, яка, на відміну від звичайних програм, ніколи не зберігає себе у вигляді окремих файлів, а також може виконувати різні небажані дії на комп'ютері.

2. **Ознаки зараження комп'ютерним 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 Windows.
- Відключення 32-розрядного допуску до диску.
- Неспроможність зберігати документи Word в інші каталоги, крім Template.
- Погана робота дисків.
- 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.

Ознаки діяльності вірусів на комп'ютерах:

• відео та аудіо ефекти (на екрані монітора несподівано чи періодично з'являються певні графічні заставки, зображення на екрані може видозмінюватися або спотворюватися, комп'ютер може програвати музичні фрагменти);

• робота на комп'ютері істотно уповільнюється;

• деякі програми не працюють або працюють неправильно;

• комп'ютер «зависає» у звичайних ситуаціях;

• вміст деяких файлів на дисках виявляється спотвореним;

• інформація на дисках втрачається;

• втрачається доступ до робочих дисків тощо. Віруси можуть проникати в обчислювальну систему двома шляхами: по-перше, з інфікованого комп'ютера при копіюванні з нього файлу, що містить вірус; по-друге, при запуску програми, розділеної між кількома комп'ютерами, в тому числі і при завантаженні операційної системи.

Зазвичай віруси розміщуються у файлах, які здебільшого керують роботою. Це файли ОС, системних і прикладних програм, драйверів пристроїв, файли об'єктних модулів і бібліотек, дисковий і системний завантажувачі, початкові тексти програм мовами високого рівня.

3. Шкідливі дії вірусів

- звукові і візуальні ефекти
- знищення інформації
- імітація збоїв ОС і апаратури
- перезавантаження комп'ютера
- розвалювання файлової системи
- передавання секретних даних через Інтернет
- масові атаки на сайти Інтернет

4. Історія виникнення вірусів

Перший прототип вірусу з'явився ще в 1971г. Програміст Боб Томас, намагаючись вирішити завдання передачі інформації з одного комп'ютера на інший, створив програму Creeper, що мимоволі «перестрибувала» з однієї машини на іншу в мережі комп'ютерного центру. Правда ця програма не «саморазмножалась», не наносила збитку.

У 1989 р. 23-річний американський студент Роберт Морріс написав невеличку програму. За його задумом програма-жарт повинна була непомітно розповсюдитися з одного комп'ютера на інший, не заважаючи їхній роботі. Але допущена в програмі помилка змусила інформацію розповсюдитися з великою швидкістю, від чого всі канали зв'язку ЕОМ виявилися перевантаженими і наукова інформація, накопичена в обчислювальних центрах, у своїй більшості стала непридатною для використання. Всього за кілька годин найважливіші мережі східного і західного узбережжя США були виведені з ладу. Епідемія охопила шість тисяч комп'ютерів, об'єднаних у 70 систем, за допомогою яких відбувався обмін найважливішою інформацією.

На сході були пошкоджені комп'ютерні центри таких великих закладів, як

Масачусетський технологічний інститут, Гарвардський, Пітсбургський, Мерілендський і Вісконсинський університети. Науково-дослідна морська лабораторія. На заході — Каліфорнійський і Стенфордський університети, науково-дослідна лабораторія НАСА, Ліверпульська лабораторія ядерних досліджень. Усі вони були зв'язані супутниковою системою «АРПАНЕТ». А причиною всього стала маленька програма-жарт, запущена в систему.

Надалі такі програми почали називати комп'ютерними вірусами.

5. КЛАСИФІКАЦІЯ ВІРУСІВ

А) За середовищем перебування

- Файлові – заражають файли *.exe, *.sys, *.dll.
- Завантажувальні (бутові, від англ. boot – завантаження) – заражають завантажувальні сектори дисків і дискет.
- Мережеві віруси – розповсюджуються через комп'ютерні мережі.

Б)За способом зараження

резидентний вірус — при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, що потім перехоплює звернення операційної системи до об'єктів зараження й впроваджується в них (перебувають у пам'яті і є активними аж до вимикання або перезавантаження комп'ютера);

- нерезидентні віруси — не заражають пам'ять комп'ютера і є активними обмежений час. Деякі віруси залишають в оперативній пам'яті невеликі резидентні програми, які не поширюють вірус;

В) За зовнішнім виглядом

- Звичайні віруси — код вірусу можна побачити на диску.
- Поліморфні – код вірусу видозмінюється.
- Невидимі віруси — використовують особливі засоби маскування і при перегляді коду вірусу не видно

Г) За можливостями

- нешкідливі — ті, які ніяк 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 й графічними, звуковими ефектами;
- небезпечні віруси — ті, які можуть призвести до серйозних збоїв у роботі, або до втрати чи пошкодження інформації;
- дуже небезпечні — ті, які можуть призвести до фізичного пошкодження обладнання (перезаписування ПЗП, виходу з ладу дискових пристроїв, пошкодження елементів материнської плати тощо);

Д) За особливостями алгоритму

- «Компаньйони-віруси» — це віруси, що не змінюють файли. Алгоритм роботи цих вірусів полягає в тому, що вони створюють для EXE-файлів файли-супутники, що мають те саме ім'я, але з розширенням .COM
- «Віруси-хробаки»— віруси, які поширюються в комп'ютерній мережі. Вони проникають у пам'ять комп'ютера з комп'ютерної мережі, встановлюють мережеві адреси інших комп'ютерів і розсилають по цих адресах свої копії;
- «Макро-віруси» — віруси цього сімейства використовують можливості макро-мов, вбудованих у системи обробки даних (текстові редактори, електронні таблиці й т.д.).
- «Троянські програми» — виконують шкідливі дії замість оголошених легальних функцій або разом з ними. Вони не спроможні до самовідтворення і передаються тільки при копіюванні користувачем. Після запуску вони зазвичай знищують себе разом з іншими файлами на диску.

6. ТИПИ АНТИВІРУСНИХ ПРОГРАМ

Для виявлення та знищення комп'ютерних вірусів використовують антивірусні програми. Всі вони поділяються на п'ять великих груп: ревізори, детектори, лікарі, фільтри, вакцини.

Тип антивірусної програми	Принцип дії
Детектори	Виявляють файли, заражені одним із відомих вірусів.
Лікарі (фаги)	Лікують заражені програми або диски, вилучаючи із заражених програм код вірусу, тобто відновлюють програму в тому стані, в якому вона була до зараження вірусом
Ревізори	Спочатку запам'ятовують відомості про стан програм і системних областей дисків . а після цього порівнюють їхній стан з початковим. При виявленні невідповідності повідомляють про неї
Фільтри	Завантажуються резидентно в оперативну пам'ять, перехоплюють ті звернення до системи, що використовуються вірусами для розмноження і нанесення шкоди, і повідомляють про них.
Вакцини	Програми, які використовуються для оброблення файлів та завантажувальних секторів з метою передчасного виявлення вірусів

Антивірусні програми групи детекторів виявляють файли, які заражені одним із відомих ним програмам вірусів.

Антивірусні програми групи лікарів (або фагів) «лікують» заражені програми або диски, видучаючи з них код вірусу, тобто відновлюючи програму в тому стані, в якому вона була до зараження вірусом.

Антивірусні програми групи ревізорів спочатку запам'ятовують відомості про стан програм і системних областей дисків, а після роботи з цими програмами порівнюють їхній стан з початковим. При виявленні невідповідності повідомляють про неї.

Антивірусні програми групи фільтрів завантажуються резидентно в оперативну пам'ять, перехоплюють ті звернення до системи, які використовуються вірусами для розмноження та нанесення шкоди і повідомляють про них.

Вакцини – програми, які використовуються для оброблення файлів та завантажувальних секторів з метою передчасного виявлення вірусів

7. Антивірусні програми

- ❑ AVP (Antiviral Toolkit Pro),
  KIS (Kaspersky Internet Security),
  KAV (Kaspersky Anti Virus) – Є. Касперский
- ❑ DrWeb – І. Данилов
- ❑ Avira
- ❑ NOD32
- ❑ Avast
- ❑ Norton Antivirus
- ❑ McAfee.

.... та інші антивірусні програми

8. Основні заходи щодо захисту від вірусів

- ❑ оснастіть свій комп'ютер однією із сучасних антивірусних програм
- ❑ користуйтеся лише перевіреними джерелами інформації
- ❑ постійно оновлюйте програмне забезпечення
- ❑ постійно обновляйте антивірусні бази