Підготував учень

Возняк Ілля

БЕЗПЕЧНИЙ ІНТЕРНЕТ

КОМП'ЮТЕРНІ ВІРУСИ

- При зараженні комп’ютера черв′як запускає HTTP сервер на випадковому TCP порту, який потім використовується для завантаження виконуваного файлу червя на інші комп’ютери.
- Черв′як отримує список IP адрес комп’ютерів, що знаходяться в мережевому оточенні зараженої машини і проводить на них атаку, що використовує уразливість переповнювання буфера MS08-067 в сервісі «Сервер» (докладніше про уразливість.

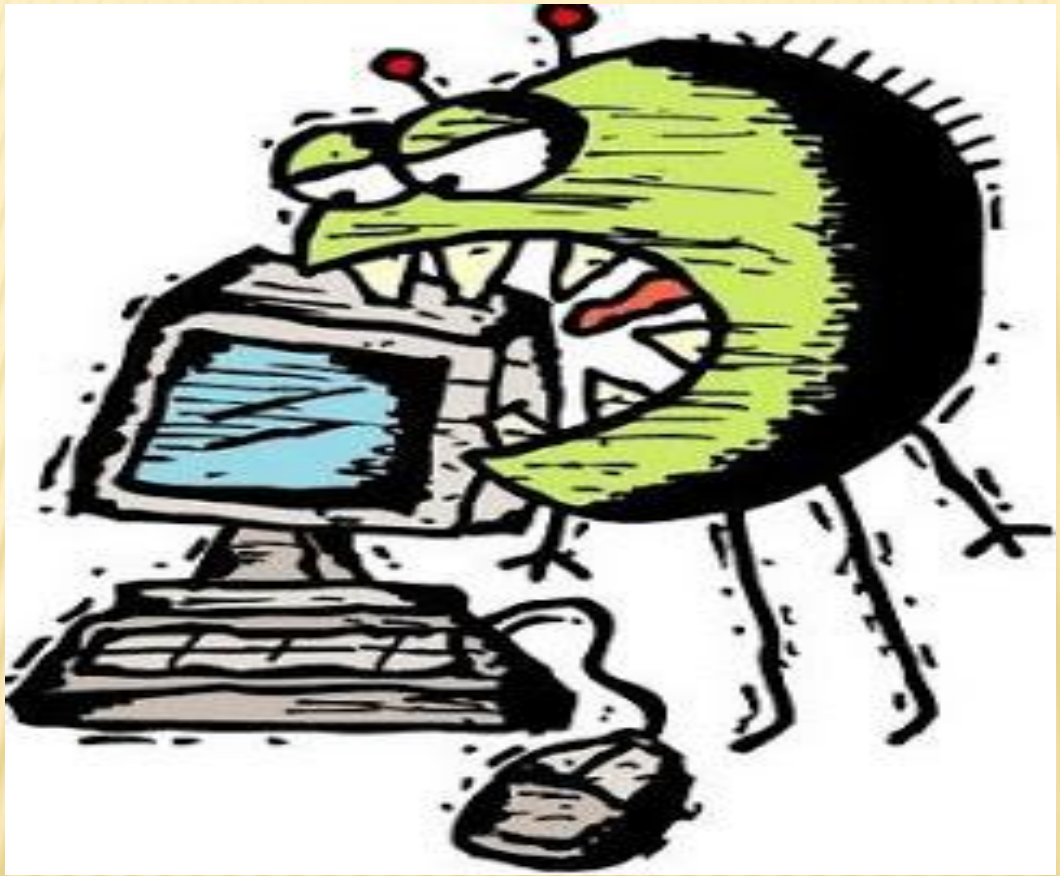
ЖИТТЄВИЙ ЦИКЛ ВІРУСУ

- Життєвий цикл вірусу

- Оскільки відмінною рисою вірусів у традиційному змісті є здатність до розмноження в рамках одного комп'ютера, розподіл вірусів на типи відбувається у відповідності зі способами розмноження.

- Сам процес розмноження може бути умовно розділений на кілька стадій:
- 1. Проникнення на комп'ютер
- 2. Активація вірусу
- 3. Пошук об'єктів для зараження
- 4. Підготовка вірусних копій
- 5. Впровадження вірусних копій

ІЛЮСТРАЦІЯ ПРОНИКНЕННЯ ВІРУСА У КОМП`ЮТЕР



ВИДИ ВІРУСІВ

- Файлові віруси
- Вірус VIENNA (Відень)
- Інші назви вірусу: 648, Restart (перезавантаження), Time Bomb (часова бомба) та ін.

- Вірус BLACK FRIDAY (Чорна п'ятниця)
- Інші назви вірусу: Israeli Virus (ізраїльський вірус), Ierusalem (Єрусалим), Black Hole (чорна дірка) та ін.

- Бутові віруси
- Вірус PING PONG (назва не потребує перекладу)
- Інші назви вірусу: Italian Bouncing (італійський стрибунець), Ball (м'ячик).

- Вірус STONED (Закам'янілий)
- Інша назва вірусу: Marijuana (Маріхуана).
- Вірус BRAIN (Мозок)

ЗАСОБИ БОРОТЬБИ З КОМП'ЮТЕРНИМИ ВІРУСАМИ

- • Регулярно робіть резервні копії важливих файлів та системних областей диска (утиліта П.Нортона Rescue, архіватори, утиліти MS-DOS Backup, Replace і т.п.). Якщо ви розробляєте власний програмний продукт, ведете базу даних тощо, візьміть за правило зберігати на окремих магнітних носіях результати своєї праці наприкінці робочого дня! Врешті-решт може просто серйозно відмовити обладнання і ви не зможете дістатися своєї інформації.
- • Якщо хтось із ваших колег демонструє на вашому комп'ютері свій продукт або ви встановлюєте нове програмне забезпечення, обов'язково перевірте його антивірусними засобами. Намагайтеся використовувати тільки законні шляхи одержання програм. Зауважимо, однак, що відомі випадки, коли і більш-менш серйозні фірми (звичайно, не злонавмисно) розповсюджували заражений продукт. Якщо ж ви працюєте на ПК "колективного користування", то перевірка комп'ютера на зараженість на початку вашого сеансу обов'язкова!
- • Для діагностування чи лікування вашого комп'ютера використовуйте тільки відомі програми, які добре зарекомендували себе. До їх числа відносяться в першу чергу ті, про які мова буде йти далі. Ще раз підкреслимо, що кожного дня з'являється у середньому 57 нових вірусів. Отже, ви повинні подбати про те, щоб у вас завжди були нові версії антивірусних програм!
- • При лікуванні комп'ютера від вірусів використовуйте чисту операційну систему, завантажуючи її з дискети. Але ж і тут, як ми казали вище, вірус може вас обманути. Захищайте дискети від записування, якщо є хоча б мала ймовірність зараження!.
- • Сучасні антивірусні програми добре документовані. У відповідних файлах, що постачаються разом із цими програмами, міститься опис усіх вірусів, з якими вони борються. Прочитайте ці файли! Ви будете мати більш повне уявлення про небезпеку, що загрожує вам і вашому комп'ютеру.

ЩО ТАКЕ МЕРЕЖЕВІ ВІРУСИ

- Мережеві віруси - це особливі програми, які поширюються через інтернет. Для цього вони використовують мережеві протоколи, загальні для всіх користувачів у всьому світі. Подібна уніфікація робить можливим стрімке розмноження і поширення програм-вбивць, що знищують корисні дані. Віруси відомі дуже давно, якщо навіть ви не проходили їх у школі на інформатиці, то на Заході вже з`явилися знамениті хакери, письменники вірусів: Морріс, Митник та їм подібні.

АНТИВІРУСНА ПРОГРАМА

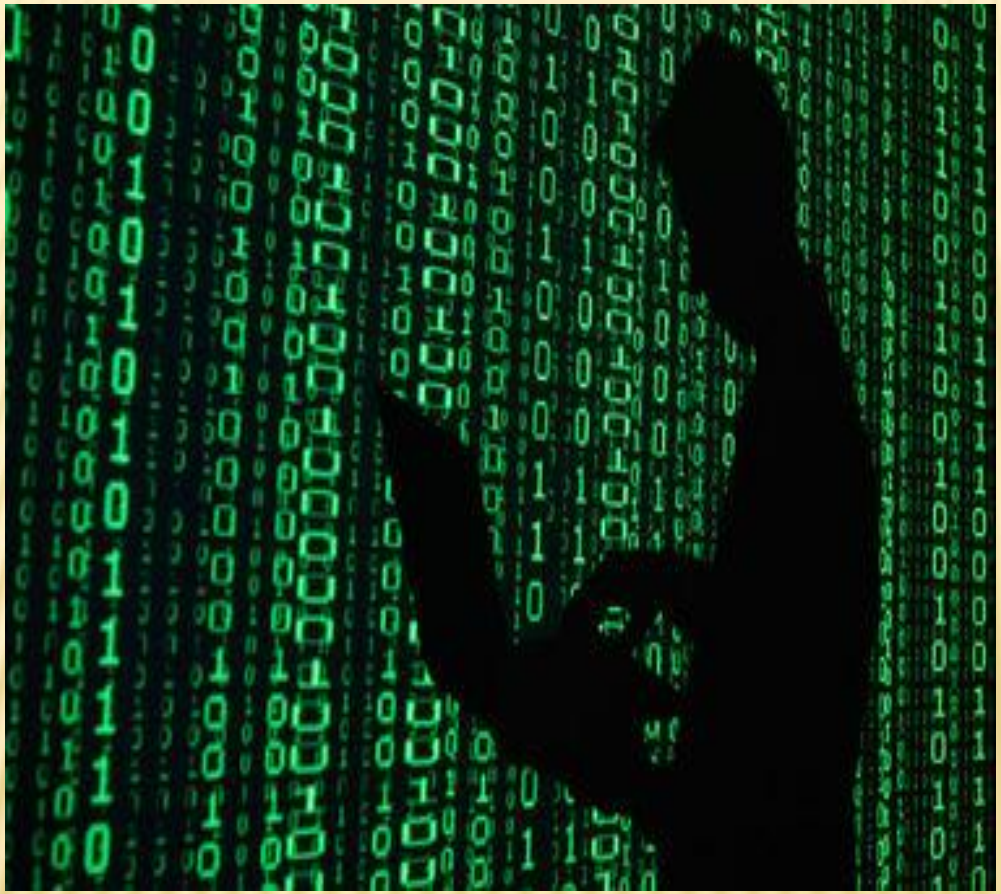
- Антивірусна програма (антивірус) — спеціалізована програма для знаходження комп'ютерних вірусів, а також небажаних (шкідливих) програм загалом та відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики — запобігання зараження (модифікації) файлів чи операційної системи шкідливим кодом.

ТИПИ АНТИВІРУСІВ

- Для боротьби з комп'ютерними вірусами розроблено декілька видів антивірусних програм: детектори, фільтри, ревізори, доктора.
- Програми-детектори виявляють конкретні віруси по сигнатурі і сигналізують про їх присутність на комп'ютері.
- Програми-ревізори виявляють присутність вірусів, періодично порівнюючи поточний стан програм, каталогів і системних областей дисків з вихідним станом.
- Програми-фільтри являють собою невеликі резидентні програми, які дозволяють виявити підозрілі дії при роботі комп'ютера, характерні для вірусів.
- Програми-доктори виявляють і видаляють віруси з оперативної пам'яті і лікують заражені вірусами файли на дисках.
- Вакцини або іммунізатори - це резидентні програми, що запобігають зараження файлів.

ФОТО АНТИВІРУСНИХ ПРОГРАМ

ЯК ЗАХИСТИТИСЯ ВІД ХАКЕРІВ І ШПИГУНІВ



ПОРАДИ

- 1. Користуйтеся складними паролями.
- 2. Користуйтесь антивірусним програмним забезпеченням.
- 3. Працюйте з комп'ютером у режимі користувача.
- 4. Виявляйте обережність при спробі підвищити власну анонімність.

КІНЕЦЬ