



Інформаційна безпека

Технічні засоби добування інформації.
Програмні засоби добування інформації.



Пригадайте:

1. Що таке інформаційна загроза?
2. Які є джерела загроз?
3. Якими шляхами поширюються загрози?
4. Які є загрози залежно від обсягів збитків?
5. Який принцип безпеки порушено, якщо було отримано доступ до керування інформаційною системою?
6. Що таке спам? Який він буває?
7. Що таке фішинг? Ddos –атака?
8. Які існують “природні” загрози?

Ви дізнаєтеся:

- Ознайомитися з технічними та програмними засобами добування інформації

«Комп'ютерне піратство»

Спроба одержати несанкціонований доступ до комп'ютерної мережі з метою ознайомитися з нею, залишити інформацію, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікується як **«комп'ютерне піратство»**.

Технічні і програмні засоби добування необхідної **інформації** - це подолання системи захисту, обмеження або заборона доступу до них посадових осіб, дезорганізації роботи технічних засобів, вивід з ладу комунікаційних і комп'ютерних мереж, усього високотехнологічного забезпечення функціонування системи управління.

Способи несанкціонованого доступу до інформації здійснюються шляхом


Застосування

- Засобів прослуховування
- Підкуп осіб, конкуруючі фірми
- фотопристроїв
- відеоапаратури
- “троянських програм”

Використання

- Недоліків мови програмування
- Переваги електро-магнітного випромінювання
- Крадіжка носіїв інформації
- Копіювання інформації
- Недоліки в операційній системі

Отримання

- Знищення даних з допомогою запитів дозволу
- Реквізитів розмежування доступу
- Використання таємних паролів

Технічні засоби добування інформації

Технічні засоби істотно розширюють і доповнюють можливості людини з добування інформації, забезпечуючи:

- a) знімання інформації з носіїв, які недоступні органам почуттів людини;
- b) добування інформації без порушення кордонів контрольованої зони;
- c) передачу інформації практично в реальному масштабі часу в будь-яку точку земної кулі;
- d) аналіз і обробку інформації в обсязі і за час, недосяжних людині;
- e) консервацію і як завгодно довгий зберігання видобутої інформації.

Класифікація пристроїв несанкціонованого зняття інформації

- За видом сигналів, що використовуються для отримання інформації
  - Акустичні
    - Мікрофонні закладні пристрої
  - Механічні
    - Стетоскопи
  - Електричні
    - Телефонні закладні пристрої
- За способом передачі інформації
  - Фізична лінія
    - Електрична мережа
    - Радіотрансляційна лінія
    - Телефонна лінія
  - Радіоканал
  - Накопичена інформація
- За часом роботи
  - Постійно функціонуючі
  - Функціонуючі за детермінованим алгоритмом
    - За заданий інтервал часу
    - При появі акустичних сигналів
    - При підніманні телефонної трубки
    - При подачі команди з пункту перехоплення
- За часом передачі інформації
  - Передачі інформації в реальному часі
  - Передачі інформації в невеликі інтервали часу з використанням апаратури стискання
- За способом електроживлення
  - З автономним електроживленням
    - Електрична мережа
    - Радіотрансляційна лінія
    - Телефонна лінія
  - З живленням від фізичної лінії

Програмні засоби добування інформації

- **Комп'ютерний вірус (КВ)**
- **Логічна бомба (ЛБ)**
- **”Троянський кінь”** (різновид ЛБ)
- **Засоби впровадження КВ і ЛБ** в інформаційні ресурси автоматизованої системи і керування ними на відстані.
- **”Нейтралізатори текстових програм”,** це програми, що забезпечують невиявлення випадкових і навмисних хиб програмного забезпечення;
- **Засоби придушення інформаційного обміну в телекомунікаційних мережах**, фальсифікації інформації в каналах ;

Шкідливе програмне забезпечення

Шкідлива програма – комп'ютерна програма або переносний код, призначений для реалізації загроз даним, що зберігаються в інформаційній системі, або для прихованого нецільового використання ресурсів системи, або іншої дії, що перешкоджає нормальному функціонуванню інформаційної системи.

- **Зловмисний програмний засіб** або **зловмисне програмне забезпечення** (англ. *Malware* - скорочення від **mal**icious - зловмисний і soft**ware** - програмне забезпечення) — програма, створена зі злими намірами.

До зловмисних програмних засобів належать віруси, рекламне ПЗ, хробаки, троянці, руткіти, клавіатурні логери, дозвонювачі, шпигунські програмні засоби, здирницькі програми, шкідливі плаґіни та інше зловмисне програмне забезпечення

Класифікація шкідливого програмного забезпечення


За наявністю матеріальної вигоди

- що не приносять пряму матеріальну вигоду тому, хто розробив (встановив) шкідливу програму:
  - жарт
  - хуліганство
  - Самоствердження, прагнення довести свою кваліфікацію
- що приносять пряму матеріальну вигоду зловмисникові:
  - крадіжка конфіденційної інформації, доступу до систем банк-клієнт, отримання PIN кодів кредитних карток тощо
  - отримання контролю над віддаленими комп'ютерними системами з метою розповсюдження спаму з численних комп'ютерів-зомбі

Комп’ютерні віруси

Комп’ютерні віруси – це спеціальні програми в машинних кодах (шкідливий програмний код) або фрагменти програм, здатні без відома та згоди користувача розмножуватися й розповсюджуватися на інші програми шляхом копіювання свого коду у файли, що зберігаються в системі.

Комп’ютерний вірус спроможний передаватися по лініях зв'язку і мережам обміну інформацією, проникати в електронні телефонні станції і системи управління. У заданий час або по сигналу вірус стирає інформацію, що зберігається в БД, або довільно змінює її.

Поняття «вірус» вживається для позначення усіх шкідливих програм, здатних «розмножуватися» , заражаючи не тільки окремі локальні комп’ютерні мережі, а й спричиняючи глобальні епідемії в Інтернеті.

Віруси - хробаки

- **Хробаки** – це один з різновидів шкідливих вірусів, що розмножуються та псують дані, збережені на комп’ютері.

- Хробаки проникають на комп'ютер-жертву без участі користувача. Хробаки використовують так звані «дірки» (уразливості) у програмному забезпеченні операційних систем, щоб проникнути на комп'ютер.

Часто хробаки розповсюджуються через файли, вкладені в електронні листи, або через деякі веб-сторінки, проте можуть також завантажуватися під час спільного користування файлами або програмами миттєвого обміну повідомленнями. Найбільш відомим представником цього класу є вірус Морріса (або "черв'як Моріса”), який вразив мережу Internet у 1988 році.

На етапі проникнення в систему хробаки діляться переважно по типах використовуваних протоколів:

- **Мережні хробаки** - хробаки, що використають для поширення протоколи Інтернет і локальні мережі.
- **Поштові хробаки** - хробаки, що поширюються у форматі повідомлень електронної пошти
- **IRC-хробаки** - хробаки, що поширюються по каналах IRC (Internet Relay Chat)
- **P2P-хробаки** - хробаки, що поширюються за допомогою пірінгових (peer-to-peer) файлообмінних мереж
- **IM-хробаки** - хробаки, що використають для поширення системи миттєвого обміну повідомленнями (IM, Instant Messenger - ICQ, MSN Messenger, AIM й ін.)

“Логічні бомби”

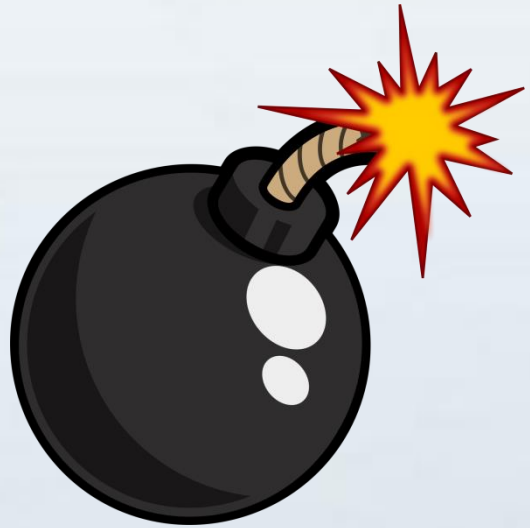
- «**Логічні бомби**» — невеликі програми, які спрацьовують з настанням певних умов і можуть призвести до часткового або повного виведення системи з ладу.

Різновидом логічної бомби є «часова бомба», яка спрацьовує в певний момент часу.

Це так звана програмна закладка, що завчасно впроваджується в інформаційні системи і мережі. Логічна бомба по сигналу, або у встановлений час, приводиться в дію, стираючи або перекручуючи інформацію в інформаційних ресурсах і виводить їх з ладу.

Це цікаво: Приклад логічної бомби

- В бібліотечній системі графства Монтгомері (Меріленд) підрядчик, якому доручили розробку комп’ютеризованої абонентської мережі, розмістив в ній логічну бомбу. При настанні певної дати ця бомба могла вивести систему із ладу, якщо замовник відмовлявся платити. Коли ж бібліотека затримала виплату грошей, підрядчик зізнався в існуванні “бомби” і пригрозив, що в разі неперерахування йому грошей він дасть “бомбі” спрацювати.



Віруси – трояни

- Одним із способів модифікації програмного забезпечення є таємне введення у програму (чужу або свою) «**троянського коня**» — команд, які дають можливість зі збереженням працездатності програми виконати додаткові, незадокументовані функції, наприклад переслати інформацію (зокрема паролі), що зберігається на комп'ютері.

- **Троян** (троянський кінь) — тип шкідливих програм, що дозволяє здійснювати схований, несанкціонований доступ до інформаційних ресурсів для добування інформації. Трояни відрізняються відсутністю механізму створення власних копій.

- Троян попадає в систему разом з вірусом або хробаком, у результаті необачних дій користувача або ж активних дій зловмисника.
- Виявити «троянського коня» дуже важко, оскільки сучасні програми складаються з тисяч і навіть мільйонів команд і мають складну структуру.

Троянські коні (Trojan Horse)

До даної групи шкідливих програм відносять:
- програми-вандали,
-«дроппери» вірусів,
- «злі жарти»,
- деякі види програм-люків;
- деякі логічні бомби,
- програми вгадування паролів;
- програми прихованого адміністрування.

Троянський кінь - одна з найнебезпечніших загроз безпеці операційних систем.

Зомбі ."Жадібні" програми

Зомбі - це програма, яка приховано під’єднується до інших підключених в Інтернет комп’ютерів, а потім використовує цей комп’ютер для запуску атак, що ускладнює відстеження шляхів до розробника програми-зомбі.

"Жадібні" програми (greedy program). - це програми, що намагаються монополізувати який-небудь ресурс, не даючи іншим програмам можливості використовувати його. Доступ таких програм до ресурсів системи призводить до порушення її доступності для інших програм.

Захоплювачі паролів

Захоплювачі паролів (password grabber) - це спеціально призначені програми для крадіжки паролів.

Утиліти схованого адміністрування (backdoor)

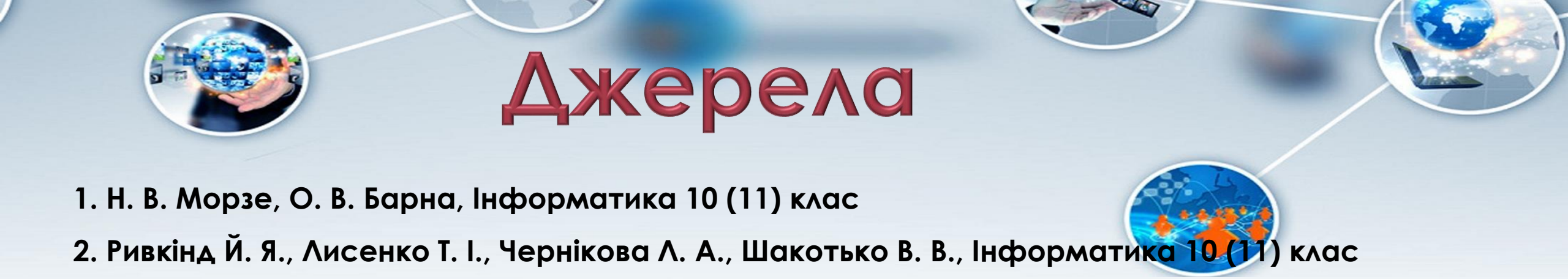
Цей вид шкідливого програмного забезпечення у деяких випадках можна віднести до групи троянських коней. Вони по своїй суті є досить могутніми утилітами віддаленого адміністрування комп'ютерів у мережі
Під час запуску троянська програма встановлює себе в системі і потім стежить за нею, при цьому користувачу не видається ніяких повідомлень про дії такого трояна в системі.

Домашнє завдання:

- Опрацювати **конспект**
- Ознайомитися з інформацією про віруси і шкідливі програми на сайті Zillya! (вірусна енциклопедія)

Додатково: Дослідити типи шкідливих програм (virus Trojan, Backdoor, Dropper, Downloader, Tool, Adware, Dialer, Worm, Exploit, Rootkit), скористайтеся даними на сайті Zillya! (вірусна енциклопедія)

Творче завдання: Засобами редактора презентацій створіть ілюстрований інтерактивний словник термінів, які виникають при захисті від можливих загроз користувача Інтернету. Передбачте, що користувач може обирати термін у списку та переходити на сторінку із тлумаченням терміна. На такій сторінці може бути ілюстрація, що відображає зміст терміна, корисне посилання на ресурс в Інтернеті, де можна детальніше ознайомитися з поняттям



Джерела

1. Н. В. Морзе, О. В. Барна, Інформатика 10 (11) клас
2. Ривкінд Й. Я., Лисенко Т. І., Чернікова Л. А., Шакотько В. В., Інформатика 10 (11) клас
3. О. О. Бондаренко, В. В. Ластовецький, О. П. Пилипчук, Є. А. Шестопалов, Інформатика 10 (11) клас
4. В. Д. Руденко, Н. В. Речич, В. О. Потієнко. Інформатика 10 (11) клас
5. http://it-science.com.ua/