**Видове вируси и техните приложения**

**Доклад от Рафи Цигаров № 2201261077 Информатика**

**Въведение**

Те са вид компютърни заплахи, които остават постоянно в паметта на компютъра и създават свои копия, което ги прави трудни за откриване и премахване.

**1.Резидентни вируси (Resident viruses)**

Резидентните вируси са тип компютърни вируси, които се инсталират и остават активни в паметта на компютъра. Те могат да работят дори когато оригиналния източник на инфекцията е ликвидиран. В зависимост от програмирането им, могат да се разделят на два вида: бързо заразни (fast infectors), които причиняват вреди бързо и са по-лесни за откриване, и бавно заразни (slow infectors), чиито симптоми се развиват постепенно.

някои от основните характеристики на резидентните вируси:

* **Постоянство**: Те остават в паметта на системата и са активни до рестартиране на компютъра.
* **Сложност при откриването**: Поради тяхната способност да се скрият в паметта, те могат да бъдат по-трудни за откриване и премахване от не-резидентните вируси.
* **Автоматично активиране**: Могат да се активират без да е необходимо да се стартира заразеният файл.
* **Инфектиране на други файлове**: След активиране, те могат да инфектират други изпълними файлове и да се разпространяват в системата.

Те се използват предимно за следните цели:

* **Непрекъснато наблюдение**: Резидентните вируси могат да мониторират действията на потребителя и да се активират при определени условия.
* **Дълготрайна инфекция**: Тъй като остават в паметта, тези вируси могат да заразяват други файлове и програми дълго време след първоначалната инфекция.
* **Избягване на откриване**: Резидентните вируси могат да се скрият от антивирусни програми, като се интегрират в системни процеси.
* **Контрол на системата**: Някои резидентни вируси могат да променят системни настройки или да блокират достъпа до определени ресурси.

**2. Вируси, инфектиращи зареждащия сектор (Boot Sector Viruses)**

Вирусите, инфектиращи зареждащия сектор, известни още като Boot Sector Viruses (BSV), заразяват зареждащия сектор на съхранителни устройства като твърди дискове и флопи дискове. Те се активират при стартиране на компютъра и могат да повредят файловата система. Съвременните варианти на тези вируси, наречени “bootkits”, се записват в Master Boot Record (MBR) и се стартират в началото на процеса на зареждане, което им позволява да скрият своето присъствие и действия.

Основни характеристики за тях са:

* **Зареждане при стартиране**: Активират се веднага при стартирането на компютъра, преди зареждането на операционната система.
* **Трудно откриване и премахване**: Тъй като се зареждат преди операционната система, те могат да бъдат трудни за откриване и премахване с обикновени антивирусни програми.
* **Разпространение**: Могат да се разпространяват чрез заразени съхранителни устройства като флопи дискове или USB устройства.
* **Последици**: Могат да причинят сериозни проблеми, като например повреда на зареждащия сектор, което може да доведе до невъзможност за стартиране на компютъра.

Приложенията на BSV са изцяло злонамерени и включват:

* **Замяна на Master Boot Record (MBR)**: BSV могат да заменят или криптират MBR, което може да попречи на нормалното зареждане на операционната система.
* **Разпространение на заразата**: След като заразят зареждащия сектор, тези вируси могат да се разпространят към всички дискове на компютъра.
* **Избягване на антивирусни програми**: Поради своята способност да се зареждат преди операционната система, BSV могат да избегнат откриването от стандартните антивирусни програми, които работят в рамките на операционната система.

**3. Вируси с директно действие**

Вирусите с директно действие са тип компютърни вируси, които се активират и изпълняват своя код веднага след стартирането. Те са сред най-простите и разпространени видове вируси. Пример за такъв вирус е Cascade.

Ето някои основни характеристики на вирусите с директно действие:

* **Бързо разпространение**: Те се разпространяват бързо, като инфектират файлове при стартирането им.
* **Лесно откриване**: Поради своята непостоянна природа, те са по-лесни за откриване от антивирусните програми.
* **Ограничен живот**: Те обикновено не остават в системата след рестартиране или изключване.

Тяхното приложение:

* **Разпространение на инфекция**: Те се размножават бързо, като заразяват голям брой файлове.
* **Увреждане на софтуера**: Могат да повредят или изтрият важни системни файлове.
* **Избягване на откриване**: Поради своята способност да се активират и деактивират бързо, те могат да избегнат откриването от антивирусни програми.

**4. Stealth вируси**

Stealth вирусите са тип компютърни вируси, които могат да скрият своето присъствие в системата. Те са известни със своята способност да избягват откриването от антивирусни програми. Пример за такъв вирус е Whale.

Ето някои характеристики на Stealth вирусите:

* **Невидимост**: Stealth вирусите често променят системни файлове и регистри, за да се скрият.
* **Затрудняване на разпознаването**: Те могат да променят своя код или да се копират в различни места, за да избегнат откриване.
* **Самосъхранение**: Stealth вирусите могат да се копират сами на различни места в системата, за да гарантират своето оцеляване при опит за премахване.

Stealth вирусите се използват за:

* **Избягване на откриване**: Те могат да се скрият от антивирусни сканирания и да останат незабелязани за дълги периоди от време.
* **Дълготрайна инфекция**: Поради способността си да се скриват, тези вируси могат да поддържат инфекцията активна дълго време.
* **Усложняване на премахването**: Stealth вирусите могат да направят процеса на премахването им изключително труден.

**5. Макро вируси**

Макро вирусите са вид компютърни вируси, които се разпространяват чрез макроси - автоматизирани скриптове, които се използват в програми като Microsoft Word и Excel. Те са известни със своята способност да се активират при отваряне на заразен документ и могат да извършват различни злонамерени действия

Характеристики

* **Автоматизация**: Макро вирусите автоматично се изпълняват, когато потребителят отвори заразен файл.
* **Скриване на действията**: Те могат да модифицират или да скрият своите действия, за да избегнат откриването от антивирусни програми.
* **Разпространение**: Лесно се разпространяват чрез споделени документи и мрежови дискове.

Макро вирусите могат да бъдат използвани за:

* **Събиране на информация**: Открадване на лични данни или корпоративна информация.
* **Разпространение на малуер**: Разпространяване на друг злонамерен софтуер в системата или мрежата.
* **Повреда на файлове**: Унищожаване или модифициране на файлове и данни.

**Заключение**

Докладът представя различни видове компютърни заплахи, които представляват сериозен риск за сигурността на информационните системи. Резидентните вируси остават активни в паметта на компютъра и могат да се скрият, като използват различни методи за инфекция и контрол на системата. Вирусите, инфектиращи зареждащия сектор, представляват опасност, като засягат най-основната част от операционната система. Вирусите с директно действие са сред най-простите, но все пак ефективни вируси, които се разпространяват бързо и могат да причинят сериозни щети на файловата система. Stealth вирусите и макро вирусите допълнително затрудняват откриването и премахването си, като използват методи за скриване и маскиране на своето присъствие.

Сигурността на информационните системи изисква постоянно внимание и усилия за защита срещу различни видове заплахи. Политики за сигурност, редовни обновления на софтуера и използването на антивирусни програми са сред основните мерки за защита срещу компютърни вируси и други видове злонамерен софтуер.