РЕФЕРАТ

ПО

Информационна сигурност

НА ТЕМА:

ВИРУСИ

Изготвил:

специалност:

СЪДЪРЖАНИЕ:

2.2.1 В зависимост от среда на обитаване

2.2.2 По начин на заразяване на средата на обитаване

2.2.3. По деструктивни възможности

2.2.4. По особеностите на алгоритъма на вируса

2.2.5. Червеи

2.2.6. Паразитни

2.2.7. Стелт - вирусите-не видимки

2.2.8. Полиморфни

2.2.9. Макро вируси

2.2.10. Троянски коне и логически бомби

2.2.11. Най-новите вируси

Компютърни вируси

1.Общи сведения за компютърните вируси

1.1 Определение за вирус

Компютърен вирус се нарича съвкупност от изпълнителен код или инструкции, която е способна да създава свои копия, не задължително съвпадащи с оригинала, и да ги внедрява в различни обекти или ресурси на компютърните системи. Копията запазват възможността си за по-нататъшно разпространение.

Вирусологът Уинфрид Глейснър дава следното определение: “Под компютърен вирус… се разбира последователност от команди, чието изпълнение предизвиква репродуциране на копие или мутация от своя код, който се намира в определена област от паметта, и което не съдържа тази последователност. Този процес се нарича инфекция. Поредицата от команди може освен това минимално изискване за самовъзпроизводимост да активира и произволни други функции.”

Предполага се, че вирусът не е самостоятелна изпълнима програма. Поредицата от команди може да е написана на Асемблер, език от високо ниво, macro език или смесена форма, от което зависи и платформената съвместимост на вируса. Под копие се разбира точното възпроизвеждане на първоначалната поредица. Областта от паметта може да бъде част от съдържанието на изпълним файл, респективно програма. Тази област се намира на външен носител, като дискета, твърд диск, CD и т.н., но може да бъде и част от оперативната памет на компютъра.С вируси могат да бъдат заразени всички програмни файлове, документи, source файове и boot sector.

1.2. Опасността от заразяване

Абсолютно никой не е застрахован от заразяване с компютърен вирус. Широкото им разпространение налага строги правила за работа с компютър, ако искате да си спестите главоболията. Абсолютно лекомислено е да си въобразявате, че "На мене това няма да ми се случи". Само в Съединените щати фирмите губят около един милиард годишно за отстраняване на последствията от заразяване. Вирусите имат на сметката си дори смъртни случаи, след като е била заразена болница в Канада. Много компании са понасяли жестоки загуби, от които понякога изобщо не са могли да се възстановят вследствие на загуба на информация поради вирус. Не случайно на въпроса се обръща все по-голямо внимание и в сериозните фирми приложенията се тестват внимателно, преди инсталация на корпоративната мрежа, потребителите имат ограничения за стартиране и/или инсталиране на приложения и т.н.

1. **3. Структура и видове вируси**

2.1. Структура на компютърен вирус

Вирусна част

Задача на вируса

Разпознаване на вируса

VirusID = ABCD

Копиране

Търси се не заразена програма, ако се намери следва инфекция

Щети

Подпрограма за нанасяне на щети

Преход

Преход в началото на програма домакин

Разпознаване на вируса. Чрез специален низ, наречен ключ, вирусът може да определи дали файлът е вече заразен. По този начин се избягва двойното заразяване.

Копираща част. Тази част на вируса търси не заразени области от паметта и се копира в програмата, подлежаща на заразяване. Тази програма може също да разпространява заразата.

Част за нанасяне на щети. При определени условия настъпва предвиденото действие.

Преход. След обработката на съответната част от командата вирусната програма се връща в началото на програмата домакин, за да може извиканата потребителска програма да започне работа.

2.2. Видове вируси

2.2.1 В зависимост от среда на обитаване

В зависимост от средата на обитаване биват мрежови, файлови и boot вируси. Както се вижда от имената им, мрежовите се разпространяват по мрежи, файловите се внедряват във файлове а boot вирусите - в boot сектора на твърдия диск или в сектора, съдържащ записа за стартиране на системата (Master Boot Record). Съществуват и комбинации, които поразяват както boot сектора, така и файлове. Обикновено подобни вируси ползват сложен алгоритъм и прилагат оригинални методи за проникване в

системата.

2.2.2 По начин на заразяване на средата на обитаване

Тук се разделят на два вида резидентни и не резидентни. При инфектиране на компютър, резидентните вируси се записват в оперативната памет резидентната си част, която прихваща обръщенията на операционната система към обектите на поразяване и се внедрява в тях. Вируси от този тип са активни до изключване или рестартиране на компютъра. Не резидентните не заразяват паметта и са активни определено време. За такива се считат и вируси, които оставят в RAM малки резидентни фрагменти, които не разпространяват вируса по- нататък.

2.2.3. По деструктивни възможности

Биват безвредни - не влияят на работата на компютъра, безопасни, ограничават се например с намаляване на дисковото пространство или звукови и графични ефекти, опасни - в състояние са да доведат до сериозни сривове на работата ви и много опасни - могат да бъдат причина за загуба на данни, унищожаване на програми, изтриване на необходима за функционирането на системата информация и т.н.

2.2.4. По особеностите на алгоритъма на вируса

Биват "компаньони" (companion), създаващи за всеки поразен *.EXE файл негов съименник с разширение COM в същата директория, който и всъщност бива стартиран, пожелаете ли да пуснете съответното приложение. *.EXE не се променя.

2.2.5. Червеи

Те са вируси, които се разпространяват по мрежите и не променят файлове или boot сектор. Те получават информация за IP адресите на други свързани машини и разпращат свои копия. Червеите понякога създават работни файлове на поразените PC-та, но могат изобщо да не се обърнат към ресурсите им (с изключение на оперативната памет).

2.2.6. Паразитни

всички не отнасящи се към горните групи вируси. Задължително променят съдържанието на дисковите сектори или файлове.

2.2.7. Стелт - вирусите-не видимки

Прихващат обръщенията на операционната система към заразени файлове или сектори и се маскират с незаразени участъци. При работа с файлове те ползват хитроумни алгоритми, позволяващи да бъдат заобиколени резидентни антивирусни монитори.

2.2.8. Полиморфни

Самошифриращи се вируси, които се откриват изключително трудно, тъй като нямат сигнатура, т.е. не съдържат постоянен код. В повечето случаи два образеца от един и същ полиморфен вирус няма да имат съвпадение. Това се реализира чрез кодиране на тялото на вируса и модификация на програмата дешифратор.

2.2.9. Макро вируси

Те ползват възможностите на макро езиците на приложния софтуер, най-често на офис пакетите. Механизмът на разпространение се основава на факта, че съществуват макрокоманди, изпълняващи се при отваряне на файла за редактиране или други операции. Като отворите заразен файл, макрокомандите поемат управлението и могат да заразят и други документи. Днес най-разпространените макро вируси за MS Office и по-конкретно за Word

2.2.10. Троянски коне и логически бомби

За разлика от компютърните вируси, на троянските коне не е нужна програма-домакин, те самите са самостоятелно приложение. Веднъж изпълнени, те изкривяват нужните им системни функции към свои собствени handler-и. Забавят локалния компютър и имат всички странични ефекти и проявления на вирусите. Проблемът при тях идва ако компютърът е включен в мрежа от локален или глобален тип. Има троянски коне, които отварят специална мрежова услуга, която може да се използва от недобросъвестни потребители за достъп до машината от разстояние. В зависимост от хардуерните възможности на системата и софтуерните възможности на троянския кон е възможно

дори подслушване на разговорите и запис на обстановката в реално време на мястото, на което се намира компютъра. Често срещана е и комбинация на троянски кон и вирус, поради което антивирусните програми сканират и за този вид програми.

Логическите бомби са специален вид троянски коне, които се активират в точно или приблизително определен момент от време или изпълнението на някакво външно условие.

2.2.11. Най-новите вируси

Възможно е да се заразите с вирус, дори без да отваряте получено съобщение по електронна поща. Разликата в новия особено неприятен тип вируси е, че действат дори без да стартирате прикрепено приложение или писмо. Засега вирусът, наречен Bubbleboy, не краде пароли и не унищожава информацията на компютъра-гостоприемник, но до появата на по-опасни и разрушителни разновидности това остава само една крачка. Най-уязвимият клиент за електронна поща от вируси от такъв тип се оказва Microsoft Outlook. Тази програма позволява да се запознаете със съдържанието на кореспонденцията си без да я отваряте, използвайки прозорец за предварителен преглед, което се оказва достатъчно за заразяване. Другите програми, в частност Exchange и Lotus Notes, също не са в състояние да защитят потребителя. След инфектиране, вирусът се само разпраща до всички, чиито адреси се съдържат в списъка на клиента з а електронна поща.

3. Вируси за различни операционни системи

Windows е най-разпространената операционна система с най-много приложения, но и най-голям брой написани вируси - няколко десетки хиляди, заедно с разновидностите. Първият вирус за Windows 2000 се появи още преди излизането на тази операционна система на бял свят. Потребителите на Linux и Unix са по-щастливи - за тази операционна система съществуват едва десетина вируса, впрочем преди година и половина броят им беше три, така че явно и тук се очаква бум. Потребителите на Linux все пак са облагодетелствани в сравнение с колегите си, работещи с Windows - по правило те нямат възможност да променят конфигурационните файлове, така че вирусът едва ли ще може да нанесе съществени поражения. Отсъствието на клиенти за електронна поща за Linux, които да са съвместими с Microsoft Outlook прави системата

устойчива на епидемии от разпространяващи се по електронната поща вируси от типа на I Love You и Kournikova. За OS/2 в днешно време за известни два вируса. Подобно е положението при набиращата популярност мултимедийна ОС BeOS. Новата мода са вирусите, предназначени за няколко операционни системи. Такъв е случаят с W32.Winux, който поразява компютри с инсталирани Linux или Windows. Инфекцията става чрез стартиране на заразен изпълним файл или отваряне на прикрепен към съобщение в електронната поща заразен файл.
Засега вирусите за мобилни телефони са истинска екзотика, но експертите очакват експанзията им да настъпи, когато 3G апаратите изместят съществуващите днес стандарти GSM и CDMA. Новостта на технологията и фактът, че стандартите за предавани по клетъчните мрежи данни все още се развиват, засега ги прави зона, свободна от вируси. Все повече производители на мобилни телефони обмислят идеята за вграждане на антивирусен продукт директно в софтуера на апарата.

4. Разпространение и действия при заразяване

4.1. Разпространение на вируси

Разпространението на вируса може да се осъществи по два начина – активно и пасивно. При активното разпространение потребителя А е предал на потребителя В една заразена програма. При това се заразява файловия хедър на В, тъй като вирусът при изпълнението си се копира най-малко в една друга програма. Този процес се обозначава като активно разпространение. Потребителят А сам е създал предпоставка за инфекция на своите файлове.

При пасивното разпространение можем да си представим следния процес: потребителят В иска да употреби софтуер на А . А му дава програмата и В я стартира на своята система. Ако програмата е била заразена, то отново В ще бъде инфектиран, но този път пасивно, защото вирусът е нямал участие със собствени процедури при пренасянето си.

Двата метода показват, че разпространението на вирусите става най-често чрез размяна или предаване на програми.

4.2. Действия при заразяване с вирус

Ако се сблъскате с компютърен вирус или подозирате, че имате този проблем, спазвайте следните прости правила:
Не се паникьосвайте и не вземайте прибързани решения. Това може да доведе не само до загуба на информация, но и до повторно заразяване.
Изключете компютъра, за да не може вирусът да продължи с разрушителната си дейност.
Всички действия по идентифицирането на типа заразяване и лечението на компютъра ЗАДЪЛЖИТЕЛНО трябва да се извършват след зареждане от чиста системна дискета.

Ако не сте уверен в силите си, не разполагате с достатъчно знания или проблемът е по-сериозен, обърнете се към по-опитен колега, системния администратор или специалист.

5. антивирусните програми

В днешно време няма начин да не обменяте информация с други потребители, било то с помощта на носители на информация или по интернет. Абсолютно реална е опасността по този начин на компютъра ви да попадне заразен файл. Коя антивирусна програма да изберете, зависи главно от следните фактори: надеждност, удобство на работа (да не "увисва" или създава технически проблеми), пълно откриване на всички разпространени типове вируси, сканиране в офис документи за макровируси, сканиране в архиви, отсъствие на фалшива тревога, възможност за изчистване на поразени файлове, актуализация. Не е лесно да се ориентирате сред множеството антивирусни скенери. Ако следите информацията в периодичния печат и интернет, ще откриете множество тестове, проведени от реномирани лаборатории, които обаче поставят на първо място различни продукти. Изводите от тези сравнения силно зависят от методиката на тестове, също и от личните предпочитания на тестващия или от фирмената политика на провелата изпитанията организация. Едва ли е добра идея да се доверите само на рекламата на фирмите производителки на антивирусен софтуер, тъй като всяка от тях твърди, че "нашият продукт е безспорен лидер, благодарение на използването на тези или онези най-нови технологии". Същото се отнася и за активността им в създаването на шум при появата на нов вирус. Злите езици твърдят, че разработчиците на антивирусни програми създават тази паника само и само да продават продуктите си.
Въпреки това трябва да направите своя избор. Ако сте потребител на Windows, без да

подценяваме достойнствата на непопадналите в тази статия продукти, прегледайте първо Norton Antivirus, McAfee VirusScan, Kaspersky Antivirus (Antiviral Toolkit Pro), Panda Antivirus, Dr. Web и F-Secure. Имайте пред вид също, че ако решите да ползвате няколко продуктите едновременно, това има своите плюсове и минуси. От една страна те ще се допълват взаимно и единият ще ви помага там, където другите са безсилни, но от друга по-често ще получавате съобщения за фалшива тревога - модули от някои антивирусни програми понякога погрешка биват интерпретирани като вируси или най-малко като съмнителни от други продукти.