**Зертханалық жұмыс №1**

**Тақырыбы:** Компьютерлік вирустер

**Жұмыстың мақсаты:**  ПК-де антивирустік программалар көмегімен компьютерлік вирустерді табу және компьютерді "емдеуді" үйрену.

1. Ақпарат дегеніміз не? Энциклопедиялық сөздікте келесі анықтама берілген - «Информация (латын. *informatio — түсіндірме*), ең бірінші – адамдармен ауызша, жазбаша немесе басқа жолмен берілетін мәлеметтер (арнайы дабылдар, техникалық жабдықтар арқылы және т.б.).

2. Ақпарат – қоршаған әлем туралы және оның ішіндегі жүріп жатқан процесстер туралы, адаммен немесе арнайы қуралдармен алынатын мәліметтер

Ақпарат қауіпсіздігі — бұл берілетін, жиналатын, өңделетін және сақталатын ақпараттың қасиеті, ақпараттың қорғаныс дәрежесін сипаттайды.

Ақпараттық қауіпсіздік адамның, қоғамның және табиғаттың қатерледен ақпараттық қорғанысын сипаттайды. Қатерлер келесілерге бөлінеді:

• Оларда бар құпияларды айту

• Олардың ақпараттық подсистемаларына ақпараттың жаман әсер ету:

• Адамның санасына және психикасына

• көп адамның санасына

• қоғамның ақпараттық ортасына

• табиғат нысандарының ақпараттық-сезу элементтеріне.

Жеке тұлғаның, қоғамның, мемлекеттің ақпараттық қауіпсіздігін қамсыздандырғанда қорғаныстың негізгі нысаны болып олардың ақпараттың ортадағы қызығушылықтары және ақпараттық құқықтары және еркіндіктері болады.

«Компьютерный вирус» термині сонғы кезде компьютерлік желілерге массалық қауып көрсететін бағдарламалар тобы. Вирустер тез көбееді және тез таралады; олармен күресу әдістерінің ретінде профилактика және анитивирустық бағдарламалар қолданылады.

Вирустер сіздің компьтеріңіздегі жұмысыңызды қиындату мүмкін. Кейбір вирустер жасырынды жұмыс істейді, сондықтан олар аса қауіпті болады – олар кездейсоқ түрде таңдалған файлдардағы сіздің деректеріңізді жасырынды түрде сізге көрінбейтіндей өзгертеді.және сіз оны ұзақ уақыт бойы байқамайсыз, бірақ олар кейін жағымсыз нәтижеге әкеледі.

Қауіпті және қызықты жағдайды келесі вирустер ұйымдастырады: олар сіздің компьютеріңізге кіріп алып, компьютеріңіздің ажырамас бқлігі болып кете алады. Мұндай вирустер жойып тастау өте қиын, егер бұл вирустерді жойып тастасаңыз жүйе мүлдем жұмыс істемей қоюы мүмкін. Мысалы ретінде файлдық-жүктеу резиденттік OneHalf вирусту көрсетуге болады, бұо стелс-вирус болып табылады және өзінің таратылуы үшін полиморфтық алгоритмдермен қолданылады.

Вирус үшін оның копиясы командаларсыз және жасырынды түрде орындалады.

Вирустерді келесі негізгі қасиеттері бойынша класстарға бөлуге болады:

|  |  |
| --- | --- |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | Өмір сүру ортасы; |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | Операциялық жүйе (OЖ); |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | Жұмыс істеу алгоритмі ; |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | Деструктивтік мүмкіндіктер. |

Өмір сүру ортасы бойынша вирустерді келесілерге бөлуге болады:

|  |  |
| --- | --- |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | файлдық; |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | Жүктелу вирустер; |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | макро; |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | желілік. |

Файлдық вирустер ір-түрлі әдістермен орындалатын командалардың ішіне кіреді (аса таралған вирустер типі), немесе сыңар-файлдар құрастырады (компаньон-вирустер), немесе файлдық жүйенің ұйымдастыруының ерекшеліктерімен қолданады (link-вирустер).

Жүктелу вирустер өздерін дисктің жүктеу секторына жазады (boot-сектор), немесе винчестердің жүйелік жүктеу аспабын сақтайтын секторына (Master Boot Record) жазылады, немесе белсенді boot-секторына бағыттаманы өзгертеді.

Макро-вирустер құжат-файлдарды және кейбір танымалы редакторлардың электронды кестелерін жұқтырады.

Желілік вирустер өздерінң таралу мақсатына жету үшін электронды поштаның және компьютерлік желілердің протоколдарымен немесе командаларымен қолданады.

Вирус жұқтырған операциялық жүйе (яғни, нысандары жұқтырылған ОЖ) вирустердің класстарға бөлінудің екінші деңгейі болып табылады. Әр файлдық немесе желілік вирус келесі тізімдегі ОЖ-дің файлдарына жұғады: OS - DOS, Windows, Win95/NT, OS/2 және т.б. Макро-вирус Word, Excel, Office97 форматтарының файлдарына жұғады.

Вирустедің жұмыс істеу алгоритмінің ерекшеліктерінің ішінен келесілерді бөлуге болады:

|  |  |
| --- | --- |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | резиденттілік; |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | стелс-алгоритмдерімен қолдану; |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | Өздік шифрлану полиморфтілік; |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | Бейстандартты тәсілдермен қолдану. |

РЕЗИДЕНТТІК вирус компьтерге вирус жұққаннан кейін оперативтік жадта өзінің резидентті бөлігін қалтырады, кейін бұл бөлік операциялық жүйенің жұқтырылған нысандарға қаратуларын өзіне қаратып олардың ішіне кіріп кетеді. Резиденттік вирустер әрдайым жадтта орналасады және компьютер өшкенге дейін белсенді болып тұрады. Резиденттік емес вирустер компьютердің жадын жұқтырмайды жіне шектелген уақыт бойы белсенділіктерін сақтайды.

Макро-вирустерді белсенді деуге болады өйткені олар әрдайым компьтердің жадында болады.

Мұндай жағдайда операциялық жүйенің ролін өзіне редактор алады.

СТЕЛС-алгоритмдермен қолдану әдістері вирустарға толық түрде немесе толық емес түрде жүйеде жасырынуға мүмкіндік береді. Файлдық стелс-вирустердің ішіндегі ең біріншісі — «Frodo» вирусы, бірінші жүктелі стелс-вирусы — «Brain».

Деструктивті мүскіндіктері бойынша вирустерді келесілерге бүлуге болады:

|  |  |
| --- | --- |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | Зиянысыз, яғни компьютердің жұмысына ешқандай зиян келтірметін вирустер ( өздерінң таралу нәтижесінде дисктегі бос орынды азайтудан басқа); |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | Қауыпты емес, бос жадтың азайуымен шектелген әсерлер көрсетеді және графикалық, дыбыстық және т.б. эффекттерді; |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | Қауіпті вирустер, компьютерде нақты жағымсыз нітижелерге әкеле аладыа; |
| C:\Documents and Settings\Администратор\Мои документы\моя работа\ОИБrus\ОИБ учебник\Picture\fieabul1.gif | Аса қауіпті, олардың жұмыс істеу алгоритмдерінде әдейі келесілерге әкелетін процедуралар жазылған: бағдарламаларды жоғалту, деректерді жою, компьютердің жұмысын қамтитын жадтың жүйелік аумақтарында жазылған ақпаратты жою және т. б. |

**Басқа "Зиянды бағдарламалар** "

«Зиянды бағдарламаларға» вирустерден басқа тағы троянды аттар (Логикалық бомбалар), intended-вирустер, вирустер конструкторлары және полиморфик-генераторлары.

Троянды аттарға кейбір бұзу амалдарын ұйымдастыратын, яғни жағдайға байланысты немесе әр іске еңгізу кезінде ақпаратты жоятын бағдарламалар.

Танымалы троянды вирустердің көбі басқа пайдалы бағдарламалардың, танымалы утилиталардың жаңа версияларының бейнелерін өздеріне алып өмір сүретін бағдарламалар.

Жиі жағдайда олар BBS-станциялары немесе электронды конференциялар арқылы таратылады. Вирустерге қарағанда троянды вирустер кең таралмайды, өйткені олар басқа бағдарламаларды жойғанда өздерінде жойып тастайды..

Intended-вирустер. Олар қателіктер мәселесінен көбее алмайды. Бұл категорияның вирустері авторлық копиядан бір рет қана көбееді Бір файлды жұқтырғаннан кейін олар көбейу қабылетін жоғалтады.

**Вирустың жұғу тәсілдері**

Файлдық вирустер вирустердің үлкен тобын құрайды. Олар орындалатын коды бар кез-келген файлдарға вирус жұқтыра алады. Бірінші кезекте .ЕХЕ және .СОМ кеңейтулері барфайлдар тұрады. Бірақ тағы оверлей файлдарыда жұқтырылуы мүмкін - .OVL. .OVI. .OVR файлдары және .SYS кеңейтуі бар драйвер. Одан басқа .ВАТ командалық файлдар.

.ЕХЕ және .СОМ файлдарына кіретін вирустердің негізгі ойлары – жүктелу файлына өздерінің кодтарын жазу. Ең қарапаым жағдайда вирус өзінің кодын файлдың соңына жазады.

2. Жүктеу вирустер дисктің жүктеу секторына зиян келтіреді, олар сектордың бір бөлігін ауыстырады немесе оған вирус жұқтырады. Бұл вирустер дисктің әр жүктелу кезінде белсенді бола бастайды, және соның арқасында компьютердегі кез-келген процессті басқара алады. Бұл вирустер көбейу жағынан аса қабілетті және жаңа дисктерге тарала алады.

Ұзақ уақыт бойы мәтіндік қауым құжатқа вирус жұға алмайды деп ойлаған. Осындай вирус ең бірінші 1995 жылдың жазында (WinWord.Concept) пайда болды және Microsoft Word for Windows 6.0 және 7.0 версияларының құжаттарын жұқтырады, олар арқылы таралады.

Вирустердің көбі бір файлды немесе жүктеу жазуын тек бір рет жұқтырады. Бұл процесстің алдында вирустер жаңа файлды алдында вирус жұқтырылмағандығын тексереді.

**Тапсырма**

Келесі файлдарда антивирустік бағдарламардың көмегімен вирустарға тексеруді ұйымдастырыңыз:

1. Орындалатын файлдармен кітапханаларда

2. DOS, EXL файлдарында .

**Бақылау сұрақтары**

1.  Компьютерлік вирус деген не?

2.   Компьютерлік вирустердің классификациясы.

3. Троянды бағдарламалар және "зиянды бағдарламалар" деген не?

4. Орандалу бағдарламаларды жұқтыру каналдары.

5. Пакеттік файлдарды жұқтыру тәсілдері.

6. Жүктеу файлдары деген не?

7. полиморфтік вирусте деген не?

8. Стелс-вирустер деп қандай вирустерді айтады?

9. Сіз білетін антивирустік бағдарламалардың артықшылықтары мен кемшіліктері?