**"КОМПЬЮТЕРИЙН ВИРУС" гэж юу вэ?**

**"ВИРУС" хэрхэн яаж vvсэж, тархав:**  
  
Анхны вирусууд тоглоомын зорилгоор vvсэж байсан бол одоо компьютерийн технологи, компьютерийн сvлжээ єргєжин тэлэхийн хэрээр вирусын зорилго нь ч улам бvр єргєн хvрээг хамрах боллоо. Аливаа вирусын гол зорилго нь єєрийгєє хэрхэн тvгээх бололцоог бий болгох (хатуу болон уян дискээр дамжих, сvлжээ, захианд хавсаргагдан тvгэх зэрэг), дараа нь тодорхой vvргийг гvйцэтгэх явдал байдаг.  
  
Эхэн vеийн вирусууд нь компьютерийн зєвхєн software хэсэг буюу программ хангамжийг гэмтээх зорилготой байсан бол сvvлийн вирусууд нь компьютерийн hardware хэсэг гэж нэрлэгддэг зарим тєхєєрємжvvд BIOS, SMOS setting, hard disk зэргийн vйлдвэрээс бичигдсэн программын хэсгийг нь єєрчлєх болон устгах чадалтай болжээ. Жишээлбэл:  
Basic Input Output System (BIOS) нь компь- ютер асах vед уншигддаг хамгийн эхний программ. Хэрвээ компьютерийн энэ хэсэг гэмтвэл компьютер асахгvй. BIOS нь motherboard дээр байрлах тодорхой микросхем буюу chip-д байрлана. Тэгвэл W95/CIH-10xx зэрэг вирусууд нь компьютерийн энэ хэсгийг гэмтээдэг.  
CMOS settings нь системийн тухай vндсэн мэдээллийг агуулна.- Энэ нь motherboard дээр байрлах тодорхой микросхем буюу chip-д байрлана. Энэхvv chip нь motherboard дээрх тусгай батерейгаар тэжээгдэх бєгєєд системийн цаг, нууц vг, уян диск, хатуу диск, CD-ROM зэрэг тєхєєрємжvvд болон бусад мэдээллийг агуулна. CMOS settings-ийг єєрчилснєєр компьютерийг асахгvй болгож болно.  
  
Зарим trojan вирусууд (Troj/KillCMOS-E г.м) CMOS settings-ийг єєрчлєх замаар компьютерийг ажиллахгvй болгоно. Ирээдvйн вирусууд нь компьютерын бусад техникийн хэсэг рvv довтлох, vvгээр зогсохгvй компьютерээр дамжуулан тухайн компьютерийг ашиглаж байгаа хvнд нєлєєлєх, жишээ нь дэлгэцийн давтамжийг єєрчилснєєр тухайн хэрэглэгчид нєлєєлєх, толгой євдvvлэх, дотор муухай оргиулах г.м боломжийг хайж байна.  
  
Vvгээр зогсохгvй санхvvгийн vйл ажиллагаанд ч вирусыг ашиглах тохиолдолд бий болж байгаа талаар бичих боллоо. Тухайлбал тухайн вирус банкны сvлжээнд нэвтрэн орж тодорхой vvрэг гvйцэтгэсний дараа єєрийгєє устгах г.м.  
  
Анхны вирусыг 1981 онд зохиогдсон гэж vздэг. Энэ нь Apple II-ийн ний дискvvдэд халдварладаг Elk Cloner гэдэг нэртэй дараах текстийг дэлгэцэнд гаргадаг байв.  
It will get on all your disks It will infiltrate your chips Yes it's Cloner! It will stick to you like glue It will modify ram too Send in the Cloner!  
  
Vvнтэй зэрэгцээд энэ вирусыг устгах зорилгоор анхны anti-virus-ийг Fridrik Skulason зохион гаргажээ. 1986 онд Пакистаны ах дvv Басит, Амжад нар уян дискийн boot sectоr-д агуулагддаг кодыг бичжээ. Энэ код нь компьютерийг уян дискнээс эхлvvлэхэд ажилладаг байв. Энэ нь єєрийнхєє кодыг хувилах чадвартай буюу санах ойд резидент болон байрлаж єєр уян дискийг компьютерт хийхэд тийшээгээ єєрийнхєє кодыг хуулдаг байв.  
  
Энэ программ нь єєрийгєє тvгээх чадвартай байсан тул vvнийг вирус гэж нэрлэжээ. Гэхдээ энэ нь зєвхєн 360KB-ийн уян дискийг л гэмтээдэг байв.  
1990 онд 200 – 500 вирус л байсан бол 1991 онд 600 - 1,000, 1992 оны сvvл гэхэд 1,000 - 2,300 virus, 1994 оны дундуур 4,500 - 7,500 virus, 1996 онд 10,000, 1998 онд 20,000 ялгаатай вирус байсан бол 2000 онд энэ тоо 50,000-ийг нэгэнт давжээ.  
  
Вирусыг ихэвчлэн вирус чухам юуг гэмтээдэг болон хэрхэн гэмтээдэг аргаар нь ангилдаг.  
Жишээлбэл вирусыг компьютерийн чухам аль хэсгийг гэмтээдэг вэ гэдэг талаас нь дараах байдлаар ангилдаг.  
  
a) System Sector virus - энэ нь компьютерийг асаах vед эхлэн ажилладаг программыг агуулсан дискийн хэсэг. Энэ талбарт бичигдсэн программыг гэмтээсэн тохиолдолд компьютер асахгvй. Компьютерт Dos Boot Sector (DBS), Partition Sector (Master Boot Record MBR) гэсэн 2 system sector байдаг. Энэ хэсэгт байрласан вирус нь компьютерийг гэмтээж ажиллахгvй болгохоос гадна уян дискээр дамжин тархах єргєн боломжтой байдаг тул тvгээмэл тохиолддог.  
  
b) File virus - энэ нь программын файлууд болох ехе, com єргєтгєлтэй файлуудыг гэмтээдэг.  
  
c) Macro virus - энэ нь data file гэж нэрлэгддэг ажлын файлууд болох word, excel, powerpoint зэрэг программуудыг ашиглан бэлтгэсэн файлуудыг гэмтээдэг. Ихэвчлэн захианд хавсаргасан файлаар дамжин тархана.  
  
d) Companion File virus - энэ нь файлуудыг гэмтээдэггvй боловч файлуудын нэр, єргєтгєлийг сольчихдог тул жинхэнэ замбараагvй байдлыг бий болгодог. Жишээ нь эдгээр нь бvх ехе файлуудыг хайн олоод com єргєтгєлтэй болгож єргєтгєлийг сольдог.  
  
e) Disk Cluster virus - энэ нь ємнєх вирустай тєсєєтэй vйлдлийг хийнэ. Гэхдээ файлын єргєтгєлийг биш харин тухайн файлуудын байрлах директоруудыг сольчихдог.  
  
f) Source Code virus - энэ нь идэвхтэй байгаа программын кодыг хайн олоод гэмтээдэг.  
  
g) Worm virus - энэ нь єєрийгєє хувилан сvлжээгээр дамжуулах чадвартай программ. Ихэвчлэн vvнийг вирусууд єєрийгєє тvгээх зорилгоор ашигладаг.  
  
Дээрх ангилалыг арай дэлгэрэнгvйгээр нь авч vзвэл:  
  
Joke Тодорхойлолт: Гэм хоргvй боловч алиа шог хэлбэрийн программууд. Ихэнх тохиолдолд хvмvvс vvнийг virus, trojan-уудтай андуурдаг.  
Vйлчилгээ: Ямар нэгэн хортой нєлєє байхгvй Нэршил: "Joke/" гэсэн vгийг агуулсан байдаг.  
  
Trojan Тодорхойлолт: Trojan-ний жинхэнэ нэршил нь Trojan Horse. Эдгээр нь янз бvрийн тоглоом, нэмэлт буюу update программуудаар дамжина. Хэсэг хугацаанд нуугдмал хэлбэрт байж байгаад тодорхой боломжийг бvрдмэгц идэвхждэг. Тухайлбал бvх файлуудыг устгах г.м  
Нэршил: "Troj/" гэсэн vгийг агуулсан байна.  
  
Access 97 macro virus Халдварлах хvрээ: MS Access 97 болон сvvлийн vеийн vйлдлийн системvvдийг гэмтээнэ.  
Ашигласан программчлалын хэл: VBA macro language.  
Vйлчилгээ: Access-ийн мэдээллийн сангийн файлуудыг гэмтээж ажиллахгvй болно.  
Нэршил: "AM97/" болон нэрэндээ "A97M", "AM" vгнvvдийг агуулсан байна.  
  
Batch file worm Халдварлах хvрээ: Сvлжээнд холбогдсон DOS, Windows 95/98/Me, Windows NT/2000 vйлдлийн систем бvхий компьютерууд.  
Vйлчилгээ: Сvлжээнд холбогдсон компьютеруудын share-ийг хайн олоод єєрєє тэнд хуулагдана.  
Нэршил: Энэ тєрлийн вирусууд нь "Bat/" гэсэн vгийг агуулсан байна.  
  
Companion virus Халдварлах хvрээ: Бvх vйлдлийн системvvд  
Vйлчилгээ: Сompanion virus нь файлуудын нэр болон єргєтлийг сольж єєр нэр єргєтгєлтэй болгодог. Жишээ нь GAME.EXE файлыг GAME.EX г.м-ээр.  
Нэршил: Албан ёсны нэршил байхгvй, ямарч нэртэй байж болно.  
  
Corel Script virus Халдварлах хvрээ: Corel SCRIPT файлууд нь бvх vйлдлийн системvvд нь ажиллах боломжтой.  
Ашигласан программчлалын хэл: Corel SCRIPT macro language.  
Vйлчилгээ: Corel SCRIPT файлуудыг гэмтээж ажиллахгvй болгоно.  
Нэршил: Энэ тєрлийн вирус нь "CSC/" vгийг агуулсан байдаг.  
  
DOS Boot Sector virus Халдварлах хvрээ: Хатуу дискийн DOS Boot Sector (DOS Boot Record) болон уйн дискийн boot sector. DOS Boot Sector virus нь Intel болон тvvнтэй зохицдог персонал компьютеруудад уян дискээр дамжин халдварлах чадвартай.  
Ашигласан программчлалын хэл нь: Intel 80x86 Assembler.  
Vйлчилгээ: Халдвар авсан компьютерийн санах ойд байрлан ямар нэгэн уян диск ашиглах vед тvvнийг гэмтээнэ.  
Нэршил: Энэ тєрлийн вирусууд нь ямар нэгэн стандарт нэршил байхгvй, ямар ч нэртэй байж болно.  
  
DOS executable file virus Халдварлах хvрээ: DOS/Windows-ийн ехе файлууд.  
Vйлчилгээ: Ехе файлуудыг гэмтээнэ. Санах ойд резидент болон байрлаж ямар нэгэн дрограммыг ажиллуулах vед тухайн программын файлуудыг гэмтээнэ. Зарим хувилбарууд нь бусад программын файлуудыг хайн олоод гэмтээдэг.  
Нэршил: Энэ тєрлийн вирусууд нь ямар нэгэн стандарт нэршил байхгvй, ямар ч нэртэй байж болно.  
  
Excel formula virus Халдварлах хvрээ: MS Excel 5 болон сvvлийн vеийн vйлдлийн системvvд.  
Ашигласан программчлалын хэл: Excel formula language.  
Vйлчилгээ: Халдвар авсан файлыг нээх vед энэ гэмтэлтэй файлыг XLSTART фолдерт хуулна. Ингэсний дараа бусад файлуудыг нээхэд энэ файл автоматаар нээгдэнэ.  
Нэршил: Энэ тєрлийн вирусууд нь "XF/", "XF97/" vгнvvдийг агуулсан байна.  
  
Excel macro virus Халдварлах хvрээ: MS Excel 5 болон сvvлийн vеийн vйлдлийн системvvд. Ашигласан программчлалын хэл: VBA3 macro language.  
Vйлчилгээ: Халдвар авсан файлыг нээх vед энэ гэмтэлтэй файлыг XLSTART фолдерт хуулна. Ингэсний дараа бусад файлуудыг нээхэд энэ файл автоматаар нээгдэнэ.  
Нэршил: "XM97/", "X97M", "XM/" гэсэн vгийг агуулна.  
  
javascript virus Халдварлах хvрээ: javascript scripting файлууд, HTML файлууд, Microsoft Outlook, Internet Explorer.  
Ашигласан программчлалын хэл: javascript  
Vйлчилгээ: Файлуудад єєрийг хуулна.  
Нэршил: "JS/" гэсэн vгийг агуулна.  
  
javascript worm Халдварлах хvрээ: javascript scripting file, HTML file, Microsoft Outlook, Internet Explorer.  
Ашигласан программчлалын хэл: javascript  
Vйлчилгээ: IRC, Outlook-ийг ашиглан электрон шуудангаар ашиглан халдвар авсан файлыг бусад хvмvvс рvv илгээнэ.  
Нэршил: "JS/" гэсэн vгийг агуулна.  
  
Linux worm Халдварлах хvрээ: Linux vйлдлийн системтэй сvлжээний компьютеруудад халдварлана.  
Vйлчилгээ: Linux worm нь сvлжээний компьютеруудад халдварлаж замаар тэднийг гэмтээнэ.  
Нэршил: "Linux/", "Unix" гэсэн vгнvvдийг агуулна.  
  
Macromedia Flash infector Халдварлах хvрээ: Macromedia Flash файлууд.  
Vйлчилгээ: Flash file-ийг ажиллуулах болгонд тvvнд єєрийгєє хуулна.  
  
Master Boot Sector virus Халдварлах хvрээ: Хатуу дискийн Master Boot Sector (Master Boot Record) болон уян дискийн boot sector. Master Boot Sector virus нь Intel болон тvvнтэй зохицдог компьютеруудыг уян диск ашиглан гэмтээж чадна.  
Ашигласан программчлалын хэл: Intel 80x86 Assembler.  
Vйлчилгээ: Гэмтэлтэй компьютерийн шуурхай санах ойд байрлаж тvvнд уян диск хийх vед тvvнийг гэмтээнэ.  
Нэршил: There is no standard naming convention for this type of virus.  
  
MIRC, pIRCH script worm Халдварлах хvрээ: IRC ашигладаг бvх системvvдэд.  
Ашигласан программчлалын хэл: IRC Script.  
Vйлчилгээ: Exe файлуудыг SCRIPT.INI файл болгон єєрчилнє.  
Нэршил: "mIRC/", "pIRC/" гэсэн vгнvvдийг агуулна Office 97 macro virus  
Халдварлах хvрээ: MS Office 97болон сvvлийн vеийн vйлдлийн системvvд.  
Ашигласан программчлалын хэл: VBA5 болон сvvлийн vеийн macro language.  
Vйлчилгээ: Word, Excel, PowerPoint, Project файлуудыг гэмтээнэ.  
Нэршил: "OF97/" гэсэн vгийг агуулна.  
  
PalmOS based executable virus Халдварлах хvрээ: PalmOS Palm (PRC) файлууд.  
Vйлчилгээ: Мэддэг бvх вирусуудыг идэвхжvvлж, бусад Palm файлуудыг гэмтээнэ.  
Нэршил: "Palm/" гэсэн vгийг агуулна.  
  
PowerPoint 97 macro virus Халдварлах хvрээ: MS PowerPoint 97 болон сvvлийн vеийн vйлдлийн системvvд.  
Ашигласан программчлалын хэл: VBA5 болон сvvлийн vеийн macro language.  
Vйлчилгээ: PowerPoint файлуудыг гэмтээхээс гадна main template (Blank Presentation.pot)-ийг гэмтээдэг ингэснээр шинэ presentation vvсгэх болгонд энэ шинээр vvссэн файл маань гэмтэнэ.  
Нэршил: "PM97/", "PP97M" гэсэн vгнvvдийг агуулна.  
  
Visual Basic Script virus Халдварлах хvрээ: Visual Basic файл, визуаль бейсик ашигласан HTML файл, Microsoft Outlook, Internet Explorer.  
Ашигласан программчлалын хэл: Visual Basic Script.  
Vйлчилгээ: Ехе файлуудыг гэмтээнэ. Зарим вирусууд жишээ нь VBS/Dismissed-B вирус нь Outlook-ийн захиануудыг гэмтээдэг.  
Нэршил: "VBS/" гэсэн vгийг агуулна.  
  
Visual Basic Script worm Халдварлах хvрээ: Visual Basic файл, визуаль бейсик ашигласан HTML файл, Microsoft Outlook, Internet Explorer.  
Ашигласан программчлалын хэл: Visual Basic Script.  
Vйлчилгээ: IRC болон Outlook-ийг ашиглан халдварласан файлыг буд тараана.  
Нэршил: "VBS/" гэсэн vгийг агуулна.  
  
Win32 executable file virus Халдварлах хvрээ: MS Windows 95/98/Me, NT, 2000 PE (Portable Executable) файлууд.  
Vйлчилгээ: Ехе файлуудыг гэмтээнэ. Зарим вирусууд жишээ нь W32/ExploreZip вирус нь Outlook-ийн захиануудыг гэмтээдэг.  
Нэршил: "W32/", "Win32" гэсэн vгнvvдийг агуулна.  
  
Win32 worm Халдварлах хvрээ: MS Windows 95/98/Me, NT, 2000 PE (Portable Executable) файлууд.  
Vйлчилгээ: Win32 worm нь Windows сvлжээний API, MAPI функцуудыг ашиглан тархах болон email client жишээ нь Microsoft Outlook-ийг ашиглан тархана. Тэдгээр нь єєрсдєє захиа бичиж тvvндээ worm программыг хавсарган илгээх чадвартай.  
Нэршил: "W32/", "Win32" гэсэн vгнvvдийг агуулна.  
  
Windows 95 executable file virus Халдварлах хvрээ: MS Windows 95/98/Me PE (Portable Executable) файлууд.  
Vйлчилгээ: Ехе файлуудыг гэмтээнэ. Зарим вирусууд нь санах ойд байрлан бусад програмуудыг ачааллах vед тэднийг гэмтээнэ. Мєн зарим нь компьютерт суугдсан программуудыг хайн олж гэмтээнэ. W95/Babylonia зэрэг зарим хувилбарууд нь захианы файлуудыг олж гэмтээдэг.  
Нэршил: "W95/", "Win95" гэсэн vгнvvдийг агуулна.  
  
Windows 98 executable file virus Халдварлах хvрээ: MS Windows 98 PE (Portable Executable) файлууд.  
Vйлчилгээ: Ехе файлуудыг гэмтээнэ. Зарим вирусууд нь санах ойд байрлан бусад програмуудыг ачааллах vед тэднийг гэмтээнэ. Мєн зарим нь компьютерт суугдсан программуудыг хайн олж гэмтээнэ.  
Нэршил: "W98/", "Win98" гэсэн vгнvvдийг агуулна.  
  
Windows NT executable file virus Халдварлах хvрээ: MS Windows NT, 2000 PE (Portable Executable) файлууд.  
Vйлчилгээ: Ехе файлуудыг гэмтээнэ.  
Нэршил: "WNT/", "WinNT" гэсэн vгнvvдийг агуулна. Windows 2000 executable file virus Халдварлах хvрээ: MS Windows 2000 PE  
  
Portable Executable файлууд.  
Халдварлах хvрээ: Ехе файлуудыг гэмтээнэ. Зарим вирусууд нь санах ойд байрлан бусад програмуудыг ачааллах vед тэднийг гэмтээнэ. Мєн зарим нь компьютерт суугдсан программуудыг хайн олж гэмтээнэ.  
Нэршил: "W2K/" гэсэн vгийг агуулна.  
  
Word macro virus Халдварлах хvрээ: MS Word-ийн бvхий л хувилбарууд.  
Ашигласан программчлалын хэл: Word Basic macro language (Word 6 ба 95-д ашигласан).  
Vйлчилгээ: Халдвартай документийг нээх vед global template (ихэвчлэн NORMAL.DOT) уруу macro-г хуулна. Ингээд бусад документийг нээх vед энэ нь автоматаар ажиллана.  
Нэршил: "WM/", "Winword", "WM97/", "W97M" гэсэн vгнvvдийг агуулна.  
  
Word 97 macro worm Халдварлах хvрээ: MS Word 97 болон бусад vйлдлийн системvvд.  
Ашигласан программчлалын хэл: VBA5 болон сvvлийн vеийн macro language. Vйлчилгээ: mail program-ууд жишээ нь MS Outlook-ийг ашиглан автоматаар гэмтэлтэй файлыг address book-д байгаа хаягуудаар илгээнэ. Зарим worm-ууд нь Word macro virus-тэй адилхан vйлчилгээтэй байдаг.  
Нэршил: "WM97/", "W97M" гэсэн vгнvvдийг агуулна.  
  
  
ВИРУС-ын учруулах хор хєнєєл  
  
  
Back Orifice Back Orifice нь Trojan-ний тєрєлд хамаарна, интернэтийн сvлжээнд холбогдох vед идэвхждэг. Оргиналь программыг Windows 95/98-д зориулан Cult of the Dead Cow (cDc) группээс 1998 оны 8 сард гаргасан. Во-2000 хувилбар нь NT-д зориулагдсан. Сvлжээг удирдахад зориулагдсан Microsoft-ийн Back Office прогрммын нэрийг бага зэрэг єєрчлєн ашигласан. TCP/IP сvлжээнд холбогдох vед ажилладаг. Гэхдээ ямар нэгэн remote компьютерээс \*!\*QWTY? команд ирэхийг хvлээнэ. Ийм командыг хvлээн авангуутаа компьютерийн тухай мэдээлэл, дискийн агуулга, архивласан болон архивыг задласан файлууд, cache-д байгаа паспортууд зэрэг нэлээд дэлгэрэнгvй мэдээллийг илгээнэ. Ингээд зогсохгvй энэ компьютерт HTTP протоколыг ашиглан web browser-ээр нэвтрэх боломжийг олгоно.  
Мєн remote компьютерт download хийх боломжийг олгоно. CIH Spacefiller Хорлон сvйтгэх чадлаараа нэлээд дээгvvрт тооцогддог энэ вирус нь 1998 оны 6 сард Chernobyl гэдэг нэрээр анх гарсан. Оргиналь вирус нь Чернобылийн сvйрэл болсон 4-р сарын 26-нд идэвхждэг. Бусад хувилбарууд нь сар болгоны 26-нд идэвхждэг. Гол аюул нь идэвхжсэн vедээ Falsh BIOS болон хатуу дискийг дахин бичихийг оролддог. Ингэснээрээ хатуу дикэн дээр файлуудыг устгаад зогсохгvй компьютерийн BIOS-ийг гэмтээснээр компьютерийг асахгvй болгоно.  
  
Kakworm Kakworm (KAK) нь worm-ийн тєрєлд хамаарна. Энэ нь Microsoft-ийн Internet Explorer browser болон Outlook Express mail program-уудаар дамжин тархана. Бусад программуудаар дамжихгvй. KAK нь HTML-ийг ашиглан захианы signature хэлбэрээр дамжина. Vvнийг харах боломжгvй. Учир нь KAK нь javascript дээр бичигдсэн байдаг. Зєвхєн энэхvv вирустай захиаг уншихад л хангалттай. Ямар нэгэн файлыг нээх болон attachment-ийг vзэх шаардлагагvй. Зєвхєн вирустэй захиаг унших vед энэ worm идэвхжиж Windows-ийг Startup фолдерт KAK.HTA файлыг хадгална. Дараагийн алхамд компьютер асахдаа KAK.HTA нь ажиллаж Windows фолдерт KAK.HTM файлыг vvсгэнэ. KAK.HTM-ийн registry-г єєрчлєх замаар бvх илгээж байгаа захиануудад signature агуулагдахаар бэлтгэнэ.  
  
Ингэснээр єєрийгєє цаашид тархах нєхцєлийг бvрдvvлнэ. Ингэсний дараа шинэ AUTOEXEC.BAT файлыг vvсгэнэ. Оргиналь файлыг нь AE.KAK-д хуулна. Ямар нэгэн сарын 1-ний єдрийн 5 цагт дэлгэцэн дээр "Kagou-Anti-Kro$oft says not today" гэсэн мэдээг гаргаад компьютерыг унтраана. Энэ нь захиагаар дамжин тархдаг вирусуудаас тархах хэлбэрээрээ хамгийн боловсронгуй болсон вирус.  
  
Laroux Laroux нь анхны Microsoft Excel macro virus буюу excel-ийн файлуудыг гэмтээдэг, энгийн macro вирус. Оригналь хувилбар нь AUTO\_OPEN болон CHECK\_FILES гэсэн 2 макрог агуулна. Эхнийх нь Exсel ажиллах vед, дараагийнх нь файл нээх vед ажиллана. CHECK\_FILES нь Excel-ийн startup path буюу эхлэх замыг хайн олоод (энэ нь ихэвчлэн XLSTART директор байна) PERSONAL.XLS-ийг ажиллуулна. Хэрэв энэ олдохгvй бол єєрєє vvнийг vvсгэнэ. PERSONAL.XLS нь Exсel-ийг ажиллуулах vед автоматаар ажилладаг (Word-ийн NORMAL.DOT-той адилхан). Хэрэв энэ файлд вирус суусан тохиолдолд Excel-ийг нээсэн хуудас болгон гэмтэх болно. Laroux нь Visual Basic-ийн макро бичихэд зориулагдсан Visual Basic for Applications (VBA) ашиглан бичигдсэн.  
  
Love Letter Энэхvv Visual Basic Script worm нь захиагаар хавсаргагдан хамгийн єргєн тархсан worm-д ордог. Энэхvv worm тархах захиа нь "ILOVEYOU" гэсэн нэртэй байх бєгєєд "kindly check the attached LOVELETTER coming from me." гэсэн vгтэй захиа байна. Ингээд хавсаргасан LOVE-LETTER-FOR-YOU.TXT.vbs файлыг нь нээвэл та энэ вирусыг єєртєє татаад авчихлаа гэсэн vг. Ингээд энэ вирус нь дараах зvйлvvдийг хийх болно.  
- IE download directory-оос WinFAT32.exe файлыг шалгаад олдвол IE-гийн Startup page-ийн registry-ийг єєрчилна. Ингэснээр дараагийн удаа компьютерийн асаах vед хэд хэдэн website-уудаас WIN-BUGSFIX.exe файлыг татан авах болно.  
- IE-гийн start page-ийг vргэлж хоосон байхаар тохируулна.  
- Компьютер асах болгонд єєрийнхєє хуулбарыг 2 газарт хуулна.  
- Outlook-ийн address book-д байгаа бvх хаягаар єєрийнхєє хуулбарыг илгээх болно.  
- Локаль болон сvлжээний бvх драйверуудаас VBS, VBE, JS, JSE, CSS, WSH, SCT, HTA файлуудыг хайн олоод бvгдэд нь єєрийнхєє кодыг бичиж VBS єргєтгєлтэй болгоно.  
- График файлууд болох JPG, JPEG файлуудыu мєн хайн олоод єєрийнхєє кодыг хуулан VBS єргєтгєлтэй болгоно.  
- Mультмедиа файлууд болох MP2, MP3 хайн олоод тэдгээрийг нуугаад оронд нь єєрийнхєє кодыг агуулсан шинэ файлыг vvсгэнэ.  
- Зарим тохиолдолд mIRC client-ийг хайн, хэрэв олдвол тvvнд HTM файлаа mIRC chat-аар илгээнэ.  
  
Melissa Melissa нь Word macro virus ба E-mail worm 2-ыг хослуулсан хувилбар. Анх 1999 оны 3-р сарын 26-нд илэрч маш тvргэн хугацаанд тархсан. Word macro virus бvхий документийг хавсаргасан захиагаар тархана. Хэрэв энэ хавсаргасан файлыг нээвэл компьютерт чинь халдварлана. Ингээд хамгийн тvрvvнд Outlook address book-ийн эхний 50 хаягаар єєрийгєє хувилан илгээнэ. Энэ захиа нь "Important Message From " нэртэй, "Here is that document you asked for ...don't show anyone else ;-)" гэсэн vгтэй захиа байна. Захианд хавсаргасан файлыг нээх vед Word-ийн NORMAL.DOC-ийг гэмтээнэ.  
  
Nimda Nimda нь virus/worm-ийн хослол. Энэ нь файлыг гэмтээхээс гадна E-mail, Web site, локал сvлжээгээр єєрийгєє тархаах чадвартай. Энэ нь EXE файлуудыг гэмтээхээс гадна Web хуудсуудыг гэмтээдэг. Мєн сvлжээний хэрэглэгчдийг хайн олоод тvvн рvv довтолдог анхны worm. Nimda нь тархахдаа дараах аргуудыг ашиглана. Сvлжээгээр E-mail-ийг ашиглан EXE файлуудыг гэмтээдэг. Мєн сvлжээний share-уудыг ашиглан тархана Хэрэв web server-т халдварласан бол энэ web server-ийн Web site-уудыг vзэх vед халдварлана.  
Дараах хувилбаруудтай:  
- File Infection. Энэ нь ехе файлуудыг хайн олоод тvvнд єєрийнхєє кодыг хуулна. Хэрэв энэ файлыг сvлжээнээс татан авч ажиллуулбал тэр нь задарч оргиналь программыг ажиллуулдаг. Ингээд єєрийнхєє vндсэн файлыг устгадаг. Хэрэв устгаагvй бол WININIT.INI-ийн командыг ашиглан Windows-ийг дараагийн удаа ажиллуулахад энэ файлыг устгадаг. Nimda нь EXE файлуудыг дараах тvлхvvрийг ашиглан хайна: [SOFTWAREMicrosoftWindowsCurrentVersionApp Paths], [SoftwareMicrosoftWindowsCurrentVersionExplorerShell Folders] Сонирхолтойн WINZIP32.EXE файл энэ вирусд гэмтдэггvй.  
  
- E-mail Worm. Бусад worm-той адилхан. E-mail client-ийн address book болон HTML файлуудаас E-mail address-уудыг хайн олоод єєрийгєє энэ хаягаар бичсэн захианд хавсарган илгээнэ. E-mail-ээр илгээсэн захиа нь 2 хэсгээс тогтно. Vvний эхнийх нь "text/html" тєрлийн MIME байна. Гэхдээ энэ нь ямар нэгэн текстийг агуулдаггvй хоосон байна. Дараагийн хэсэг нь "audio/x-wav"тєрлийн MIME байх бєгєєд README.EXE программыг хавсаргасан байна. Зарим программууд тухайлбал Microsoft Internet Explorer 5.5 SP1-ийг хэрэглэгч нар нь хvрэлцэн ирсэн HTML захианд хавсаргасан файлыг автоматаар нээдэг. Ингэснээр захианд хавсаргасан файл ажиллаж компьютерт халдварлана. Nimda нь єєрийн SMTP server-ийг ашиглан E-mail захиа илгээнэ.  
  
- Web Worm. Nimda нь интернэтээр Microsoft IIS Web server-vvдийг хайна. Хэрэв сервер олдвол Nimda нь дурын Web хуудсанд нэвтрэн тvvнийг javascript-ийг ашиглан єєрчилдєг. Энэ код нь Web browser-ээс README.EML-ийг нээх vед ажиллана.  
  
- File Share Propagation. Локал сvлжээний share-уудыг хайна. Хэрэв олдвол Nimda hidden/system файл (RICHED20.DLL)-ийг дамжуулна. Word, WordPad, Outlook зэрэг программыг ажиллуулахад RICHED20.DLL автоматаар ажиллах болно.  
  
Pretty Park Энэ нь worm, Trojan-ний хослол. Анх 1999 оны 6 сард илэрсэн. Олон хувилбаруудтай. E-mail захианд хавсаргасан PRETTY PARK.EXE файлаар дамжин тархана. Эхний удаа ажиллуулахад санах ойд єєрийгєє хуулна. Дараа нь Windows-ийн System дотор FILES32.VXD файлд єєрийгєє хуулна. Мєн ямар нэгэн exe файлыг ажиллуулсан бол тvvний registry-ийг єєрчилнє. Ингээд єєрийгєє задлаж компьютерт суулгана. Хэрэв энд ямар нэгэн алдаа гарвал 3D Pipes screen saver (SSPIPES.SCR)-ийг ажиллуулахыг оролдоно. Хэрэв энэ олдохгvй бол CANALISATION3D.SCR screen saver-ийг ажиллуулна. Интернэтэд холбогдсоны дараа 30 сек-д болгонд routing хийхийг оролдох болно. Ингэсний vр дvнд дараах 13 IRC chat серверийн аль нэгэнтэйн холбоо тогтоохыг оролдоно. irc.twiny.net irc.stealth.net irc.grolier.net irc.club-internet.fr ircnet.irc.aol.com irc.emn.fr irc.anet.com irc.insat.com irc.ncal.verio.net irc.cifnet.com irc.skybel.net irc.eurecom.fr irc.easynet.co.uk Холбоо тогтоосны дараа системийн мэдээллийг илгээх болно. Мєн 30 минут болгонд roiting хийхийг оролдоно. Ингэхдээ Outlook-ийн address book-ийг ашиглан єєрийг хавсаргасан захиаг илгээнэ. Захиа нь "C:CoolProgsPretty Park.exe" нэртэй байхаас гадна worm бvхий ехе файлыг хавсаргасан байна.  
  
W32.SirCam 2001-07-21-нд анх илэрсэн worm. Windows-ийн бvх хувилбарт халдварладаг. Захианд хавсаргасан файл болон дотоод сvлжээгээр тархана. Melissa вирустай адилхан mailbox-ийг ашиглан олсон eamil хаяг болгон уруу захиа илгээх чадвартай. Англи испани 2 хувилбартай. Ихэнх захианы эцсийн ба эхинй єгvvлбэрт дараах vгнvvдийг ашиглана.  
Испани хувилбарт: Hola como estas ? Nos vemos pronto, gracias.  
Англи хувилбарт: Hi! How are you? See you later. Thanks  
Энэ 2 єгvvлбэрийн хооронд дараах текстvvд байна.  
Испани хувилбарт: Te mando este archivo para que me des tu punto de vista Espero me puedas ayudar con el archivo que te mando Espero te guste este archivo que te mando Este es el archivo con la informaci=n que me pediste  
Англи хувилбарт: I send you this file in order to have your advice I hope you can help me with this file that I send I hope you like the file that I sendo you. This is the file with the information that you ask for.  
Хавсаргах файл нь .bat, .com, .lnk, .pif, .doc, .xls, .zip г.м єргєтгєлтэй дурын файл байна. Энэ файлыг нээвэл дараах байдлаар идэвхжинэ.  
- C:WindowsTemp болон C:Recycled-д энэхvv файлыг хуулна. Хэрэв энэ файл нь dоc єргєтгєлтэй бол word-ийг, єєр єргєтгєлтэй бол тухайн файлыг ажиллуулдаг программыг ажиллуулахад идэвхжинэ. Ингээд єєрийгєє C:RecycledSirc32.exe ба C:WindowsSystemScam32.exe уруу хуулна.  
- Дараах 2 registry key-г єєрчилнє. HKEY\_LOCAL\_MACHINESoftwareMicrosoftWindowsCurrentVersionRunServices Driver32="SCam32.exe" HKEY\_CLASSES\_ROOTexefileshellopen command=""C:  
ecycledSirC32.exe""%1" %\*" Эхний registry-ийг єєрчилснєєр windows ажиллаж эхэлмэгц энэ worm ажиллах боломжийг бvрдvvлнэ. Харин 2 дахь registry-ийг єєрчилснєєр энэ worm ямар нэгэн ехе файлыг ажиллуулах vед ажиллах боломжийг бvрдvvлнэ.  
- Дараа нь дараах registry-ийг шинээр vvсгэнэ: HKEY\_LOCAL\_MACHINESoftwareSirCam Энэ worm сvлжээний share-уудыг ашиглан дотоод сvлжээгээр хурдан тархана. Энэ тохиолдолд сvлжээнд холбогдсон бусад компьютеруудын хувьд дараах vйлдлийг хийхийг оролдоно.  
- RecycledSirc32.exe-д єєрийгєє хуулна.  
- Autoexec.bat-д "@win  
ecycledsirc32.exe" гэсэн мєрийг нэмнэ.  
- WindowsRundll32.exe-ийг C:WindowsRun32.exe уруу хуулна.  
- Windows  
undll32.exe-ийг C:RecycledSirc32.exe-ээр солино. Зарим тохиолдолд (33-аас 1 тохиолдолд нь) дараах vйлдлийг гvйцэтгэнэ:  
- C:RecycledSirc32.exe-ийг C:WindowsScmx32.exe уруу хуулна.  
- HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionExplorerShellFoldersStartup-д "Microsoft Internet Office.exe"-г хуулна. Зарим тохиолдолд (20-оос 1 тохиолдолд буюу ихэвчлэн 10 сарын 26-нд) С дискний бvх файлыг устгана. Зарим тохиолдолд (33-аас 1 тохиолдолд нь) C:RecycledSircam.sys-д дараах текстийг нэмэх замаар дискийг дvvргэнэ.  
- [SirCam\_2rp\_Ein\_NoC\_Rma\_CuiTzeO\_MicH\_MeX]  
  
- [SirCam Version 1.0 Copyright ¬ 2000 2rP Made in / Hecho en - Cuitzeo, Michoacan Mexico] Энэ worm SMTP-ийг ашиглан email илгээх чадвартай. Ингэхдээ email-ийн хаягийг дараах 2 аргаар олно. Эхлээд дараах registry key-г ашиглан email хаяг олж авна.  
- HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionExplorerShell FoldersCache болон  
- HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionExplorerShell FoldersPersonal Эдгээрийг ашиглан олсон sho\*., get\*., hot\*., \*.htm файлуудаас email хаягуудыг олж %system%sc?1.dll файлд хуулна. scy1.dll-д %cache%sho\*., hot\*., get\*-ээс олсон хаягуудыг, sch1.dll-д %personal%sho\*., hot\*., get\*-ээс олдсон хаягуудыг, sci1.dll-д %cache%\*.htm-ээс олдсон хаягуудыг, sc.dll-д %personal%\*.htm-ээс олдсон хаягуудыг тус тус хуулна.  
  
Мєн %system%-ийн бvх дэд фолдеруудаас \*.wab (Windows Address Books-ын файл) файлуудыг олж email хаягуудыг нь %system%scw1.dll уруу хуулна. Ингээд дараах registry-ийг ашиглан .doc, .xls, .zip тєрлийн файлуудыг олж нэрсийг нь %system%scd.dll-д хуулна.  
- HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionExplorerShell FoldersPersonal болон  
- HKEY\_CURRENT\_USERSoftwareMicrosoftWindowsCurrentVersionExplorerShell FoldersDesktop  
- эдгээр олдсон .doc, .xls, .zip файлуудад worm єєрийнхєє кодыг хуулна. Ингээд захиа бичнэ. Ингэхдээ From: талбарт registry-ээс олдсон email хаягийг тавина. Хэрэв захиа илгээгч Испани хэлийг ашигладаг бол испани хувилбарыг, бусад тохиолдолд англи хувилбарыг ашиглана. Захианд хавсаргах файлаа scd.dll дэх жагсаалтаас сонгоно.  
  
Энэ вирусыг устгах заавар:  
- Интернэтийн болон дотоод сvлжээнээс компьютерээ салгана.  
- HKEY\_LOCAL\_MACHINESoftwareMicrosoftWindowsCurrentVersionRunServicesDriver32-ийн утгыг устгана.  
- HKEY\_LOCAL\_MACHINESoftwareSirCam-ийг устгана.  
- HKEY\_CLASSES\_ROOTexefileshellopencommand-ийн утгыг "%1" %\* болгон єєрчилнє. (хашилт-хувь-нэг-хашилт, хоосон зай, хувь, од) энэ бол Default утга.  
- RecycledSircam.sys, RecycledSirc32.exe (Windows Recycle Bin дотор байгаа) болон WindowsSystemSCam32.exe файлуудыг устгана.  
- Autoexec.bat файлын "@win   
ecycledsirc32.exe" мєрийг устгана.  
W32.Sircam.Worm@mm халдварласан- файлуудыг илрvvлж устгана.  
- run32.exe файлыг rundll32.exe файл болгон нэрийг нь солино.  
  
  
ВИРУС-аас хэрхэн хамгаалах   
  
a) Юуны ємнє antivirus программаа байнга update хийх замаар шинэчилж байх хэрэгтэй.  
b) Ихэнх antivirus программ нь уян дискэн дээр safe boot disk-ийг бэлтгэдэг. Энэ нь компьютерийн boot вирустсэн тохиолдолд гаднаас уншуулан boot-ийн вирусыг устгахад зориулагдсан байдаг тул ийм дискийг урьдчилан бэлтгэсэн байвал сайн. Учир нь нэгэнт вирустсэн тохиолдолд єєрийн тань ашиглаж байгаа antivirus тухайн вирусыг таньж устгаж чадаагvй гэсэн vг, тэгэхээр компьютер вирустсэний дараа энэ дискийг бэлтгэх нь ач холбогдол багатай. Учир нь ихэнх вирусууд antivirus-ний эсрэг тодорхой хэмжээний довтолгоог хийхээр зориулагдсан байж болно.  
  
c) Зарим вирусууд компьютерийн boot уруу довтолж системийн файлыг гэмтээснээр компьютерийг ажиллахгvй болгодог. Иймээс урьдчилан hard boot disk буюу системийн дискийг бэлтгэсэн байвал сайн.  
d) Word-ийн doc, Excel-ийн xls файлуудыг гаднаас хуулахыг аль болох хийхгvй байвал сайн. Учир нь эдгээр файлуудаар macro вирус дамжих єргєн боломжтой байдаг. Шаардлагатай тохиолдолд тухайн файлаа RDF єргєтгєлтэй болговол энэ тєрлийн файлаар macro вирус дамждаггvй.  
  
e) Хэрэв єєрєє л сайн мэдэхгvй байгаа бол элдэв хvнээс ирсэн захианд хавсаргасан файлыг нээж vзэхгvй байхыг зєвлєж байна. Учир нь ихэнх worm захианд хавсаргасан файлаар дамждаг.  
f) Уян диск нь єєрийн протекттэй байдаг. Хэрэв уян дискээс файл хуулан авахыг хvсэж байвал уян дискний протектийг байнга ашиглаж байхыг зєвлєж байна. Энэ нь найдвартай хамгаалалт болж чаддаггvй ч зарим тохиолдолд тус болдог.  
  
g) Vргэлж ашигладаг программуудынхаа инсталлыг хадгалж байх хэрэгтэй. Мєн тvvнчлэн компьютерийнхээ driver дискvvдийг мєн адил.  
h) Vvнээс гадна хамгийн найдвартай арга бол vргэлж backup хийх. Хийсэн ажлын файлуудынхаа хуулбарыг сайн бэлтгэж байх нь хэзээд илvvдэхгvй гэдгийг байнга санаж байх хэрэгтэй.  
  
Хамгийн єргєн ашиглагдаж байгаа Anti-Virus-ийн программууд:  
KAV - http://www.kaspersky.com/  
NOD32 - http://www.eset.com/  
BiTDeFeNDeR - http://www.bitdefender.com/  
aVaST! Anti-Virushttp://avast.com/  
AntiViral Toolkit Pro - http://www.avp.com/  
- http://www.avp.ch/  
- http://www.avp.tm/  
- http://www.avp.ru/  
F-Prot - http://www.complex.is/  
F-Prot - Professional http://www.commandcom.com/  
http://www.DataFellows.com/  
- Integrity Master http://www.stiller.com/  
McAfee VirusScan - http://www.nai.com/  
MIMESweeper (mail firewall)- http://www.mimesweeper.com/  
Norman- Virus Control http://www.norman.com/  
- Norton Anti-virus, Symantec Anti-virus for Mac http://www.symantec.com/  
Trend Micro- (PC-Cillin, InterScan, Scanmail, Serverprotect) http://www.antivirus.com/  
Sophos- Sweep http://www.sophos.com/