Хавсралт В.

КОМПЬЮТЕРИЙН ВИРУС

Компьютерт зөвшөөрөлгүйгээр нэвтрэх чадвартай, тодорхой үүрэг, зорилготой программыг вирус гэж ойлгож болно. Өөрөөр хэлбэл вирус нь хэрэглэгчид мэдэгдэлгүйгээр, түүний зөвшөөрөлгүй компьютерт нэвтэрч чаддаг, мөн тодорхой үүргийг биелүүлэх чадвартай байна. Жишээлбэл: зарим вирус exe файлуудыг гэмтээдэг бол, зарим нь компьютерийн санах ойд байрлан файлыг өөрчлөх болон шинээр файлууд үүсгэдэг г.м төрөл бүрийн зорилготой байдаг. Анхны вирусууд тоглоомын зорилгоор үүсэж байсан бол одоо компьютерийн технологи, компьютерийн сүлжээ өргөжин тэлэхийн хэрээр вирусын зорилго нь ч улам бүр өргөн хүрээг хамрах боллоо. Аливаа вирусын гол зорилго нь өөрийгөө хэрхэн түгээх бололцоог бий болгох (хатуу болон уян дискээр дамжих, сүлжээ, захианд хавсаргагдан түгэх зэрэг), дараа нь тодорхой үүргийг гүйцэтгэх явдал байдаг. Эхэн үеийн вирусууд нь компьютерийн зөвхөн software хэсэг буюу программ хангамжийг гэмтээх зорилготой байсан бол сүүлийн вирусууд нь компьютерийн hardware хэсэг гэж нэрлэгддэг зарим төхөөрөмжүүд BIOS, SMOS setting, hard disk зэргийн үйлдвэрээс бичигдсэн программын хэсгийг нь өөрчлөх болон устгах чадалтай болжээ. Жишээлбэл:

- Basic Input Output System (BIOS) нь компьютер асах үед уншигддаг хамгийн эхний программ. Хэрвээ компьютерийн энэ хэсэг гэмтвэл компьютер асахгүй. 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 үндсэн мэдээллийг агуулна. Энэ нь motherboard дээр байрлах тодорхой микросхем буюу chip-д байрлана. Энэхүү chip нь motherboard дээрх тусгай батерейгаар тэжээгдэх бөгөөд системийн цаг, нууц үг, уян диск, хатуу диск, CD-ROM зэрэг төхөөрөмжүүд болон бусад мэдээллийг агуулна. CMOS settings-ийг өөрчилснөөр компьютерийг асахгүй болгож болно. Зарим trojan вирусууд (Troj/KillCMOS-E г.м) CMOS settings-ийг өөрчлөх замаар компьютерийг ажиллахгүй болгоно.

Ирээдүйн вирусууд нь компьютерын бусад техникийн хэсэг рүү довтлох, үүгээр зогсохгүй компьютерээр дамжуулан тухайн компьютерийг ашиглаж байгаа хүнд нөлөөлөх, жишээ нь дэлгэцийн давтамжийг өөрчилснөөр тухайн хэрэглэгчид нөлөөлөх, толгой өвдүүлэх, дотор муухай оргиулах г.м боломжийг хайж байна. Үүгээр зогсохгүй санхүүгийн үйл ажиллагаанд ч вирусыг ашиглах тохиолдолд бий болж байгаа талаар бичих боллоо. Тухайлбал тухайн вирус банкны сүлжээнд нэврэн орж тодорхой үүрэг гүйцэтгэсний дараа өөрийгөө устгах г.м.

Анхны вирусыг 1981 онд зохиогдсон гэж үздэг. Энэ нь Apple II-ийн ний дискүүдэд 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!
```

Үүнтэй зэрэгцээд энэ вирусыг устгах зорилгоор анхны anti-virus-ийг Fridrik Skulason зохион гаргажээ.

1986 онд Пакистаны ах дүү Басит, Амжад нар уян дискийн boot sector-д агуулагддаг кодыг бичжээ. Энэ код нь компьютерийг уян дискнээс эхлүүлэхэд ажилладаг байв. Энэ нь өөрийнхөө кодыг хувилах чадвартай буюу санах ойд резидент болон байрлаж өөр уян дискийг компьютерт хийхэд тийшээгээ өөрийнхөө кодыг хуулдаг байв. Энэ программ нь өөрийгөө дүгээх чадвартай байсан тул үүнийг вирус гэж нэрлэжээ. Гэхдээ энэ нь зөвхөн 360KB-ийн уян дискийг л гэмтээдэг байв.

1990 онд 200 – 500 вирус л байсан бол 1991 онд 600 - 1,000, 1992 оны сүүл 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.

а) System Sector virus - энэ нь компьютерийг асаах үед эхлэн ажилладаг программыг агуулсан дискийн хэсэг. Энэ талбарт бичигдсэн программыг гэмтээсэн тохиолдолд компьютер асахгүй. Компьютерт Dos Boot Sector (DBS), Partition Sector (Master Boot Record MBR) гэсэн 2 system sector

байдаг. Энэ хэсэгт байрласан вирус нь компьютерийг гэмтээж ажиллахгүй болгохоос гадна уян дискээр дамжин тархах өргөн боломжтой байдаг тул түгээмэл тохиолддог.

b) File virus – энэ нь программын файлууд болох exe, com өргөтгөлтэй 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 гэмтээдэггүй боловч файлуудын нэр, өргөтгөлийг сольчихдог тул жинхэнэ замбараагүй байдлыг бий болгодог. Жишээ нь эдгээр нь бүх exe файлуудыг хайн олоод com өргөтгөлтэй болгож өргөтгөлийг сольдог.

e) Disk Cluster virus – энэ нь өмнөх вирустай төсөөтэй үйлдлийг хийнэ. Гэхдээ файлын өргөтгөлийг 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 өөрийгөө хувилан сүлжээгээр дамжуулах чадвартай программ. Ихэвчлэн үүнийг вирусууд өөрийгөө түгээх зорилгоор ашигладаг.

Дээрх ангилалыг арай дэлгэрэнгүйгээр нь авч үзвэл:

Joke

Тодорхойлолт:

Гэм хоргүй боловч алиа шог хэлбэрийн программууд. Ихэнх тохиолдолд хүмүүс үүнийг virus, trojan-уудтай андуурдаг.

Үйлчилгээ:

Ямар нэгэн хортой нөлөө байхгүй

Нэршил:

"Joke/" гэсэн үгийг агуулсан байдаг.

Trojan

Тодорхойлолт:

Trojan-ний жинхэнэ нэршил нь Trojan Horse. Эдгээр нь янз бүрийн тоглоом, нэмэлт буюу update программуудаар дамжина. Хэсэг хугацаанд нуугдмал хэлбэрт байж байгаад тодорхой боломжийг бүрдмэгц идэвхждэг. Тухайлбал бүх файлуудыг устгах г.м

Нэршил:

"Troj/" гэсэн үгийг агуулсан байна.

Access 97 macro virus

Халдварлах хүрээ:

MS Access 97 болон сүүлийн үеийн үйлдлийн системүүдийг гэмтээнэ.

Ашигласан программчлалын хэл:

VBA macro language.

Үйлчилгээ:

Access-ийн мэдээллийн сангийн файлуудыг гэмтээж ажиллахгүй болно.

Нэршил:

"AM97/" болон нэрэндээ "A97M", "AM" үгнүүдийг агуулсан байна.

Batch file worm

Халдварлах хүрээ:

Сүлжээнд холбогдсон DOS, Windows 95/98/Me, Windows NT/2000 үйлдлийн систем бүхий компьютерууд.

Үйлчилгээ:

Сүлжээнд холбогдсон компьютеруудын share-ийг хайн олоод өөрөө тэнд хуулагдана.

Нэршил:

Энэ төрлийн вирусууд нь "Bat/" гэсэн үгийг агуулсан байна.

Companion virus

Халдварлах хүрээ:

Бүх үйлдлийн системүүд

Үйлчилгээ:

Companion virus нь файлуудын нэр болон өргөтлийг сольж өөр нэр өргөтгөлтэй болгодог. Жишээ нь GAME.EXE файлыг GAME.EX г.м-ээр.

Нэршил:

Албан ёсны нэршил байхгүй, ямарч нэртэй байж болно.

Corel Script virus

Халдварлах хүрээ:
Corel SCRIPT файлууд нь бүх үйлдлийн системүүд нь ажиллах боломжтой.
Ашигласан программчлалын хэл:
Corel SCRIPT macro language.
Үйлчилгээ:
Corel SCRIPT файлуудыг гэмтээж ажиллахгүй болгоно.
Нэршил:
Энэ төрлийн вирус нь "CSC/" үгийг агуулсан байдаг.

DOS Boot Sector virus
Халдварлах хүрээ:
Хатуу дискийн DOS Boot Sector (DOS Boot Record) болон уйн дискийн boot sector.
DOS Boot Sector virus нь Intel болон түүнтэй зохицдог персонал компьютеруудад уян дискээр дамжин халдварлах чадвартай.
Ашигласан программчлалын хэл нь:
Intel 80x86 Assembler.
Үйлчилгээ:
Халдвар авсан компьютерийн санах ойд байрлан ямар нэгэн уян диск ашиглах үед түүнийг гэмтээнэ.
Нэршил:
Энэ төрлийн вирусууд нь ямар нэгэн стандарт нэршил байхгүй, ямар ч нэртэй байж болно.

DOS executable file virus
Халдварлах хүрээ:
DOS/Windows-ийн exe файлууд.
Үйлчилгээ:
Exe файлуудыг гэмтээнэ. Санах ойд резидент болон байрлаж ямар нэгэн дрограммыг ажиллуулах үед тухайн программын файлуудыг гэмтээнэ. Зарим хувилбарууд нь бусад программын файлуудыг хайн олоод гэмтээдэг.
Нэршил:
Энэ төрлийн вирусууд нь ямар нэгэн стандарт нэршил байхгүй, ямар ч нэртэй байж болно.

Excel formula virus
Халдварлах хүрээ:
MS Excel 5 болон сүүлийн үеийн үйлдлийн системүүд.
Ашигласан программчлалын хэл:
Excel formula language.
Үйлчилгээ:
Халдвар авсан файлыг нээх үед энэ гэмтэлтэй файлыг XLSTART фолдерт хуулна. Ингэсний дараа бусад файлуудыг нээхэд энэ файл автоматаар нээгдэнэ.
Нэршил:
Энэ төрлийн вирусууд нь "XF/", "XF97/" үгнүүдийг агуулсан байна.

Excel macro virus
Халдварлах хүрээ:
MS Excel 5 болон сүүлийн үеийн үйлдлийн системүүд.
Ашигласан программчлалын хэл:
VBA3 macro language.
Үйлчилгээ:
Халдвар авсан файлыг нээх үед энэ гэмтэлтэй файлыг XLSTART фолдерт хуулна. Ингэсний дараа бусад файлуудыг нээхэд энэ файл автоматаар нээгдэнэ.
Нэршил:
"XM97/", "X97M", "XM/" гэсэн үгийг агуулна.

JavaScript virus
Халдварлах хүрээ:
JavaScript scripting файлууд, HTML файлууд, Microsoft Outlook, Internet Explorer.
Ашигласан программчлалын хэл:
JavaScript
Үйлчилгээ:
Файлуудад өөрийг хуулна.
Нэршил:
"JS/" гэсэн үгийг агуулна.

JavaScript worm
- Халдварлах хүрээ:
  - JavaScript scripting file, HTML file, Microsoft Outlook, Internet Explorer.
- Ашигласан программчлалын хэл:
  - JavaScript
- Үйлчилгээ:
  - IRC, Outlook-ийг ашиглан электрон шуудангаар ашиглан халдвар авсан файлыг бусад хүмүүс рүү илгээнэ.
- Нэршил:
  - "JS/" гэсэн үгийг агуулна.

Linux worm
- Халдварлах хүрээ:
  - Linux үйлдлийн системтэй сүлжээний компьютеруудад халдварлана.
- Үйлчилгээ:
  - Linux worm нь сүлжээний компьютеруудад халдварлаж замаар тэднийг гэмтээнэ.
- Нэршил:
  - "Linux/", "Unix" гэсэн үгнүүдийг агуулна.

Macromedia Flash infector
- Халдварлах хүрээ:
  - Macromedia Flash файлууд.
- Үйлчилгээ:
  - Flash file-ийг ажиллуулах болгонд түүнд өөрийгөө хуулна.

Master Boot Sector virus
- Халдварлах хүрээ:
  - Хатуу дискийн Master Boot Sector (Master Boot Record) болон уян дискийн boot sector. Master Boot Sector virus нь Intel болон түүнтэй зохицдог компьютеруудыг уян диск ашиглан гэмтээж чадна.
- Ашигласан программчлалын хэл:
  - Intel 80x86 Assembler.
- Үйлчилгээ:
  - Гэмтэлтэй компьютерийн шуурхай санах ойд байрлаж түүнд уян диск хийх үед түүнийг гэмтээнэ.
- Нэршил:
  - There is no standard naming convention for this type of virus.

MIRC, pIRCH script worm
- Халдварлах хүрээ:
  - IRC ашигладаг бүх системүүдэд.
- Ашигласан программчлалын хэл:
  - IRC Script.
- Үйлчилгээ:
  - Exe файлуудыг SCRIPT.INI файл болгон өөрчилнө.
- Нэршил:
  - "mIRC/", "pIRC/" гэсэн үгнүүдийг агуулна

Office 97 macro virus
- Халдварлах хүрээ:
  - MS Office 97болон сүүлийн үеийн үйлдлийн системүүд.
- Ашигласан программчлалын хэл:
  - VBA5 болон сүүлийн үеийн macro language.
- Үйлчилгээ:
  - Word, Excel, PowerPoint, Project файлуудыг гэмтээнэ.
- Нэршил:
  - "OF97/" гэсэн үгийг агуулна.

PalmOS based executable virus
- Халдварлах хүрээ:
  - PalmOS Palm (PRC) файлууд.
- Үйлчилгээ:
  - Мэддэг бүх вирусуудыг идэвхжүүлж, бусад Palm файлуудыг гэмтээнэ.
- Нэршил:
  - "Palm/" гэсэн үгийг агуулна.

PowerPoint 97 macro virus

Халдварлах хүрээ:
MS PowerPoint 97 болон сүүлийн үеийн үйлдлийн системүүд.
Ашигласан программчлалын хэл:
VBA5 болон сүүлийн үеийн macro language.
Үйлчилгээ:
PowerPoint файлуудыг гэмтээхээс гадна main template (Blank Presentation.pot)-ийг гэмтээдэг ингэснээр шинэ presentation үүсгэх болгонд энэ шинээр үүссэн файл маань гэмтэнэ.
Нэршил:
"PM97/", "PP97M" гэсэн үгнүүдийг агуулна.

Visual Basic Script virus
Халдварлах хүрээ:
Visual Basic файл, визуаль бейсик ашигласан HTML файл, Microsoft Outlook, Internet Explorer.
Ашигласан программчлалын хэл:
Visual Basic Script.
Үйлчилгээ:
Exe файлуудыг гэмтээнэ. Зарим вирусууд жишээ нь VBS/Dismissed-B вирус нь Outlook-ийн захианууудыг гэмтээдэг.
Нэршил:
"VBS/" гэсэн үгийг агуулна.

Visual Basic Script worm
Халдварлах хүрээ:
Visual Basic файл, визуаль бейсик ашигласан HTML файл, Microsoft Outlook, Internet Explorer.
Ашигласан программчлалын хэл:
Visual Basic Script.
Үйлчилгээ:
IRC болон Outlook-ийг ашиглан халдварласан файлыг бусдад тараана.
Нэршил:
"VBS/" гэсэн үгийг агуулна.

Win32 executable file virus
Халдварлах хүрээ:
MS Windows 95/98/Me, NT, 2000 PE (Portable Executable) файлууд.
Үйлчилгээ:
Exe файлуудыг гэмтээнэ. Зарим вирусууд жишээ нь W32/ExploreZip вирус нь Outlook-ийн захианууудыг гэмтээдэг.
Нэршил:
"W32/", "Win32" гэсэн үгнүүдийг агуулна.

Win32 worm
Халдварлах хүрээ:
MS Windows 95/98/Me, NT, 2000 PE (Portable Executable) файлууд.
Үйлчилгээ:
Win32 worm нь Windows сүлжээний API, MAPI функцуудыг ашиглан тархах болон email client жишээ нь Microsoft Outlook-ийг ашиглан тархана. Тэдгээр нь өөрсдөө захиа бичиж түүндээ worm программыг хавсарган илгээх чадвартай.
Нэршил:
"W32/", "Win32" гэсэн үгнүүдийг агуулна.

Windows 95 executable file virus
Халдварлах хүрээ:
MS Windows 95/98/Me PE (Portable Executable) файлууп.
Үйлчилгээ:
Exe файлуудыг гэмтээнэ. Зарим вирусууд нь санах ойд байрлан бусад програмуудыг ачааллах үед тэднийг гэмтээнэ. Мөн зарим нь компьютерт суугдсан программуудыг хайн олж гэмтээнэ.
W95/Babylonia зэрэг зарим хувилбарууд нь захианы файлуудыг олж гэмтээдэг.
Нэршил:
"W95/", "Win95" гэсэн үгнүүдийг агуулна.

Windows 98 executable file virus
Халдварлах хүрээ:

MS Windows 98 PE (Portable Executable) файлууд.

Үйлчилгээ:

Exe файлуудыг гэмтээнэ. Зарим вирусууд нь санах ойд байрлан бусад програмуудыг ачааллах үед тэднийг гэмтээнэ. Мөн зарим нь компьютерт суугдсан программуудыг хайн олж гэмтээнэ.

Нэршил:

"W98/", "Win98" гэсэн үгнүүдийг агуулна.

Windows NT executable file virus

Халдварлах хүрээ:

MS Windows NT, 2000 PE (Portable Executable) файлууд.

Үйлчилгээ:

Exe файлуудыг гэмтээнэ.

Нэршил:

"WNT/", "WinNT" гэсэн үгнүүдийг агуулна.

Windows 2000 executable file virus

Халдварлах хүрээ:

MS Windows 2000 PE (Portable Executable) файлууд.

Халдварлах хүрээ:

Exe файлуудыг гэмтээнэ. Зарим вирусууд нь санах ойд байрлан бусад програмуудыг ачааллах үед тэднийг гэмтээнэ. Мөн зарим нь компьютерт суугдсан программуудыг хайн олж гэмтээнэ.

Нэршил:

"W2K/" гэсэн үгийг агуулна.

Word macro virus

Халдварлах хүрээ:

MS Word-ийн бүхий л хувилбарууд.

Ашигласан программчлалын хэл:

Word Basic macro language (Word 6 ба 95-д ашигласан).

Үйлчилгээ:

Халдвартай документийг нээх үед global template (ихэвчлэн NORMAL.DOT) уруу macro-г хуулна. Ингээд бусад документийг нээх үед энэ нь автоматаар ажиллана.

Нэршил:

"WM/", "Winword", "WM97/", "W97M" гэсэн үгнүүдийг агуулна.

Word 97 macro worm

Халдварлах хүрээ:

MS Word 97 болон бусад үйлдлийн системүүд.

Ашигласан программчлалын хэл:

VBA5 болон сүүлийн үеийн macro language.

Үйлчилгээ:

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 үйлчилгээтэй байдаг.

Нэршил:

"WM97/", "W97M" гэсэн үгнүүдийг агуулна.

Өнөөдөр дараах вирусууд хамгийн их хор нөлөөг үзүүлж байна.

Back Orifice

Back Orifice нь Trojan-ний төрөлд хамаарна, интернэтийн сүлжээнд холбогдох үед идэвхждэг. Оргиналь программыг Windows 95/98-д зориулан Cult of the Dead Cow (cDc) группээс 1998 оны 8 сард гаргасан. Bo-2000 хувилбар нь NT-д зориулагдсан. Сүлжээг удирдахад зориулагдсан Microsoft-ийн Back Office прогрммын нэрийг бага зэрэг өөрчлөн ашигласан. TCP/IP сүлжээнд холбогдох үед ажилладаг. Гэхдээ ямар нэгэн remote компьютерээс *!*QWTY? команд ирэхийг хүлээнэ. Ийм командыг хүлээн авангуутаа компьютерийн тухай мэдээлэл, дискийн агуулга, архивласан болон архивыг задласан файлууд, cache-д байгаа паспортууд зэрэг нэлээд дэлгэрэнгүй мэдээллийг илгээнэ. Ингээд зогсохгүй энэ компьютерт HTTP протоколыг ашиглан web browser-ээр нэвтрэх боломжийг олгоно. Мөн remote компьютерт download хийх боломжийг олгоно.

CIH Spacefiller

Хорлон сүйтгэх чадлаараа нэлээд дээгүүрт тооцогддог энэ вирус нь 1998 оны 6 сард Chernobyl гэдэг нэрээр анх гарсан.

Оргиналь вирус нь Чернобылийн сүйрэл болсон 4-р сарын 26-нд идэвхждэг. Бусад хувилбарууд нь сар болгоны 26-нд идэвхждэг. Гол аюул нь идэвхжсэн үедээ Falsh BIOS болон хатуу дискийг дахин бичихийг оролддог. Ингэснээрээ хатуу дикэн дээр файлуудыг устгаад зогсохгүй компьютерийн BIOS-ийг гэмтээснээр компьютерийг асахгүй болгоно.

Kakworm

Kakworm (KAK) нь worm-ийн төрөлд хамаарна. Энэ нь Microsoft-ийн Internet Explorer browser болон Outlook Express mail program-уудаар дамжин тархана. Бусад программуудаар дамжихгүй.

KAK нь HTML-ийг ашиглан захианы signature хэлбэрээр дамжина. Үүнийг харах боломжгүй. Учир нь KAK нь JavaScript дээр бичигдсэн байдаг. Зөвхөн энэхүү вирустай захиаг уншихад л хангалттай. Ямар нэгэн файлыг нээх болон attachment-ийг үзэх шаардлагагүй. Зөвхөн вирустэй захиаг унших үед энэ worm идэвхжиж Windows-ийг Startup фолдерт KAK.HTA файлыг хадгална. Дараагийн алхамд компьютер асахдаа KAK.HTA нь ажиллаж Windows фолдерт KAK.HTM файлыг үүсгэнэ. KAK.HTM-ийн registry-г өөрчлөх замаар бүх илгээж байгаа захианууддад signature агуулагдахаар бэлтгэнэ. Ингэснээр өөрийгөө цаашид тархах нөхцөлийг бүрдүүлнэ. Ингэсний дараа шинэ \AUTOEXEC.BAT файлыг үүсгэнэ. Оргиналь файлыг нь \AE.KAK-д хуулна. Ямар нэгэн сарын 1-ний өдрийн 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 Excel ажиллах үед, дараагийнх нь файл нээх үед 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 олдохгүй бол өөрөө үүнийг үүсгэнэ. PERSONAL.XLS нь Excel-ийг ажиллуулах үед 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

Энэхүү Visual Basic Script worm нь захиагаар хавсаргагдан хамгийн өргөн тархсан worm-д ордог. Энэхүү worm тархах захиа нь "ILOVEYOU" гэсэн нэртэй байх бөгөөд "kindly check the attached LOVELETTER coming from me." гэсэн үгтэй захиа байна. Ингээд хавсаргасан LOVE-LETTER-FOR-YOU.TXT.vbs файлыг нь нээвэл та энэ вирусыг өөртөө татаад авчихлаа гэсэн үг.

Ингээд энэ вирус нь дараах зүйлүүдийг хийх болно.

- IE download directory-ооc WinFAT32.exe файлыг шалгаад олдвол IE-гийн Startup page-ийн registry-ийг өөрчилна. Ингэснээр дараагийн удаа компьютерийн асаах үед хэд хэдэн website-уудаас WIN-BUGSFIX.exe файлыг татан авах болно.
- IE-гийн start page-ийг үргэлж хоосон байхаар тохируулна.
- Компьютер асах болгонд өөрийнхөө хуулбарыг 2 газарт хуулна.
- Outlook-ийн address book-д байгаа бүх хаягаар өөрийнхөө хуулбарыг илгээх болно.
- Локаль болон сүлжээний бүх драйверуудаас VBS, VBE, JS, JSE, CSS, WSH, SCT, HTA файлуудыг хайн олоод бүгдэд нь өөрийнхөө кодыг бичиж VBS өргөтгөлтэй болгоно.
- График файлууд болох JPG, JPEG файлуудыu мөн хайн олоод өөрийнхөө кодыг хуулан VBS өргөтгөлтэй болгоно.
- Мультмедиа файлууд болох MP2, MP3 хайн олоод тэдгээрийг нуугаад оронд нь өөрийнхөө кодыг агуулсан шинэ файлыг үүсгэнэ.

- Зарим тохиолдолд mIRC client-ийг хайн, хэрэв олдвол түүнд 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 түргэн хугацаанд тархсан. Word macro virus бүхий документийг хавсаргасан захиагаар тархана. Хэрэв энэ хавсаргасан файлыг нээвэл компьютерт чинь халдварлана. Ингээд хамгийн түрүүнд Outlook address book-ийн эхний 50 хаягаар өөрийгөө хувилан илгээнэ. Энэ захиа нь "Important Message From <your username>" нэртэй, "Here is that document you asked for ...don't show anyone else ;-)" гэсэн үгтэй захиа байна. Захианд хавсаргасан файлыг нээх үед Word-ийн NORMAL.DOC-ийг гэмтээнэ.

Nimda

Nimda нь virus/worm-ийн хослол. Энэ нь файлыг гэмтээхээс гадна E-mail, Web site, локал сүлжээгээр өөрийгөө тархаах чадвартай. Энэ нь EXE файлуудыг гэмтээхээс гадна Web хуудсуудыг гэмтээдэг. Мөн сүлжээний хэрэглэгчдийг хайн олоод түүн рүү довтолдог анхны worm. Nimda нь тархахдаа дараах аргуудыг ашиглана.

Сүлжээгээр E-mail-ийг ашиглан EXE файлуудыг гэмтээдэг. Мөн сүлжээний share-уудыг ашиглан тархана

Хэрэв web server-т халдварласан бол энэ web server-ийн Web site-уудыг үзэх үед халдварлана. Дараах хувилбаруудтай:

- File Infection. Энэ нь exe файлуудыг хайн олоод түүнд өөрийнхөө кодыг хуулна. Хэрэв энэ файлыг сүлжээнээс татан авч ажиллуулбал тэр нь задарч оргиналь программыг ажиллуулдаг. Ингээд өөрийнхөө үндсэн файлыг устгадаг. Хэрэв устгаагүй бол WININIT.INI-ийн командыг ашиглан Windows-ийг дараагийн удаа ажиллуулахад энэ файлыг устгадаг. Nimda нь EXE файлуудыг дараах түлхүүрийг ашиглан хайна:

  [SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths],

  [Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders]

  Сонирхолтойн WINZIP32.EXE файл энэ вирусд гэмтдэггүй.

- E-mail Worm. Бусад worm-той адилхан. E-mail client-ийн address book болон HTML файлуудаас E-mail address-уудыг хайн олоод өөрийгөө энэ хаягаар бичсэн захианд хавсарган илгээнэ. E-mail-ээр илгээсэн захиа нь 2 хэсгээс тогтно. Үүний эхнийх нь "text/html" төрлийн MIME байна. Гэхдээ энэ нь ямар нэгэн текстийг агуулдаггүй хоосон байна. Дараагийн хэсэг нь "audio/x-wav"төрлийн MIME байх бөгөөд README.EXE программыг хавсаргасан байна. Зарим программууд тухайлбал Microsoft Internet Explorer 5.5 SP1-ийг хэрэглэгч нар нь хүрэлцэн ирсэн HTML захианд хавсаргасан файлыг автоматаар нээдэг. Ингэснээр захианд хавсаргасан файл ажиллаж компьютерт халдварлана. Nimda нь өөрийн SMTP server-ийг ашиглан E-mail захиа илгээнэ.

- Web Worm. Nimda нь интернэтээр Microsoft IIS Web server-үүдийг хайна. Хэрэв сервер олдвол Nimda нь дурын Web хуудсанд нэвтрэн түүнийг JavaScript-ийг ашиглан өөрчилдөг. Энэ код нь Web browser-ээс README.EML-ийг нээх үед ажиллана.

- File Share Propagation.

  Локал сүлжээний 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 өөрийгөө хуулна. Дараа нь Windows-ийн System дотор FILES32.VXD файлд өөрийгөө хуулна. Мөн ямар нэгэн exe файлыг ажиллуулсан бол түүний registry-ийг өөрчилнө.

Ингээд өөрийгөө задлаж компьютерт суулгана. Хэрэв энд ямар нэгэн алдаа гарвал 3D Pipes screen saver (SSPIPES.SCR)-ийг ажиллуулахыг оролдоно. Хэрэв энэ олдохгүй бол CANALISATION3D.SCR screen saver-ийг ажиллуулна.

Интернэтэд холбогдсоны дараа 30 сек-д болгонд routing хийхийг оролдох болно. Ингэсний үр дүнд 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.

Мөн 30 минут болгонд roiting хийхийг оролдоно. Ингэхдээ Outlook-ийн address book-ийг ашиглан өөрийг хавсаргасан захиаг илгээнэ. Захиа нь "C:\CoolProgs\Pretty Park.exe" нэртэй байхаас гадна worm бүхий exe файлыг хавсаргасан байна.

W32.SirCam

2001-07-21-нд анх илэрсэн worm. Windows-ийн бүх хувилбарт халдварладаг. Захианд хавсаргасан файл болон дотоод сүлжээгээр тархана. Melissa вирустай адилхан mailbox-ийг ашиглан олсон eamil хаяг болгон уруу захиа илгээх чадвартай. Англи испани 2 хувилбартай. Ихэнх захианы эцсийн ба эхинй өгүүлбэрт дараах үгнүүдийг ашиглана.

Испани хувилбарт: Hola como estas ? Nos vemos pronto, gracias.

Англи хувилбарт: Hi! How are you? See you later. Thanks

Энэ 2 өгүүлбэрийн хооронд дараах текстүүд 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 өргөтгөлтэй дурын файл байна. Энэ файлыг нээвэл дараах байдлаар идэвхжинэ.

- C:\Windows\Temp\ болон C:\Recycled\-д энэхүү файлыг хуулна. Хэрэв энэ файл нь doc өргөтгөлтэй бол word-ийг, өөр өргөтгөлтэй бол тухайн файлыг ажиллуулдаг программыг ажиллуулахад идэвхжинэ. Ингээд өөрийгөө C:\Recycled\Sirc32.exe ба C:\Windows\System\Scam32.exe уруу хуулна.
- Дараах 2 registry key-г өөрчилнө.

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\

  Driver32="<Windows System>\SCam32.exe"

  HKEY_CLASSES_ROOT\exefile\shell\open\

  command=""C:\recycled\SirC32.exe""%1" %*"

  Эхний registry-ийг өөрчилснөөр windows ажиллаж эхэлмэгц энэ worm ажиллах боломжийг бүрдүүлнэ. Харин 2 дахь registry-ийг өөрчилснөөр энэ worm ямар нэгэн exe файлыг ажиллуулах үед ажиллах боломжийг бүрдүүлнэ.

- Дараа нь дараах registry-ийг шинээр үүсгэнэ:

  HKEY_LOCAL_MACHINE\Software\SirCam

Энэ worm сүлжээний share-уудыг ашиглан дотоод сүлжээгээр хурдан тархана. Энэ тохиолдолд сүлжээнд холбогдсон бусад компьютеруудын хувьд дараах үйлдлийг хийхийг оролдоно.

- <Computer>\Recycled\Sirc32.exe-д өөрийгөө хуулна.
- <Computer>\Autoexec.bat-д "@win\recycled\sirc32.exe" гэсэн мөрийг нэмнэ.
- <Computer>\Windows\Rundll32.exe-ийг C:\Windows\Run32.exe уруу хуулна.
- <Computer>\Windows\rundll32.exe-ийг C:\Recycled\Sirc32.exe-ээр солино.

Зарим тохиолдолд (33-аас 1 тохиолдолд нь) дараах үйлдлийг гүйцэтгэнэ:

- C:\Recycled\Sirc32.exe-ийг C:\Windows\Scmx32.exe уруу хуулна.
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellFolders\Start up-д "Microsoft Internet Office.exe"-г хуулна.

Зарим тохиолдолд (20-оос 1 тохиолдолд буюу ихэвчлэн 10 сарын 26-нд) C дискний бүх файлыг устгана.

Зарим тохиолдолд (33-аас 1 тохиолдолд нь) C:\Recycled\Sircam.sys-д дараах текстийг нэмэх замаар дискийг дүүргэнэ.

- [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_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache болон
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal

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, sct1.dll-д %personal%*.htm-ээс олдсон хаягуудыг тус тус хуулна. Мөн %system%-ийн бүх 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 төрлийн файлуудыг олж нэрсийг нь %system%\scd.dll-д хуулна.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal болон
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop
- эдгээр олдсон .doc, .xls, .zip файлуудад worm өөрийнхөө 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 сүлжээнээс компьютерээ салгана.
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Driver32-ийн утгыг устгана.
- HKEY_LOCAL_MACHINE\Software\SirCam-ийг устгана.
- HKEY_CLASSES_ROOT\exefile\shell\open\command-ийн утгыг "%1" %* болгон өөрчилнө. (хашилт-хувь-нэг-хашилт, хоосон зай, хувь, од) энэ бол Default утга.

- Recycled\Sircam.sys, Recycled\Sirc32.exe (Windows Recycle Bin дотор байгаа) болон Windows\System\SCam32.exe файлуудыг устгана.
- Autoexec.bat файлын "@win \recycled\sirc32.exe" мөрийг устгана.
- W32.Sircam.Worm@mm халдварласан файлуудыг илрүүлж устгана.
- run32.exe файлыг rundll32.exe файл болгон нэрийг нь солино.

Вирусээс хэрхэн хамгаалах талаар дараах зөвлөлгөөг өгье.

a) Юуны өмнө 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 өөрийн тань ашиглаж байгаа antivirus тухайн вирусыг таньж устгаж чадаагүй гэсэн үг, 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 ажиллахгүй болгодог. Иймээс урьдчилан hard boot disk буюу системийн дискийг бэлтгэсэн байвал сайн.

d) Word-ийн doc, Excel-ийн xls файлуудыг гаднаас хуулахыг аль болох хийхгүй байвал сайн. Учир нь эдгээр файлуудаар macro вирус дамжих өргөн боломжтой байдаг. Шаардлагатай тохиолдолд тухайн файлаа RDF өргөтгөлтэй болговол энэ төрлийн файлаар macro вирус дамждаггүй.

e) Хэрэв өөрөө л сайн мэдэхгүй байгаа бол элдэв хүнээс ирсэн захианд хавсаргасан файлыг нээж үзэхгүй байхыг зөвлөж байна. Учир нь ихэнх worm захианд хавсаргасан файлаар дамждаг.

f) Уян диск нь өөрийн протекттэй байдаг. Хэрэв уян дискээс файл хуулан авахыг хүсэж байвал уян дискний протектийг байнга ашиглаж байхыг зөвлөж байна. Энэ нь найдвартай хамгаалалт болж чаддаггүй ч зарим тохиолдолд тус болдог.

g) Үргэлж ашигладаг программуудынхаа инсталлыг хадгалж байх хэрэгтэй. Мөн түүнчлэн компьютерийнхээ driver дискүүдийг мөн адил.

h) Үүнээс гадна хамгийн найдвартай арга бол үргэлж backup хийх. Хийсэн ажлын файлуудынхаа хуулбарыг сайн бэлтгэж байх нь хэзээд илүүдэхгүй гэдгийг байнга санаж байх хэрэгтэй.

Хамгийн өргөн ашиглагдаж байгаа Anti-Virus-ийн программууд

- 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/