UNIVERSIDAT DE VALENCIA

ESCOLA UNIVERSITARIA D´ESTUDIS EMPRESARIALS

DEPARTAMENT DE DIRECCIÓ D´EMPRESES

INFORMÀTICA APLICADA A LA GESTIÓ D´EMPRESES

Curs 1998-99

Virus

Informatics

Salvador Climent Serrano

VIRUS INFORMÀTICS

El primer indici de definició de virus informàtic apareix l'any 1949 per John Von Neuman en l'article "Teoria i organització d'un autòmat complicat" on exposa la seua teoria de programes amb capacitat de multliplicarse.

Deu anys després als laboratoris *AT & T* Bell inventen el joc de guerra nuclear (*Core Wars*) o guerra de nuclis, consistia en una batalla entre els codis de dos programadors, en la que cada jugador desenrotllava un programa la missió del qual era la d'acaparar la màxima memòria possible mitjançant la reproducció de sí mateix . En esta lluita cada un dels programes intentava destruir a l'oponent i després d'un període de temps guanyava qui tinguera la major quantitat de memòria ocupada al seu oponent amb el seu programa.

El terme "Virus " tal com ho entenem hui apareix en 1983 on *Fred Cohen* ho va definir en la seua tesi doctoral com " Un programa que pot infectar altres programes modificant-los per a incloure una versió de si mateix".

Als anys 86-87 és quan es produïx l'explosió del fenomen virus en PCs i va ser en l'entorn universitari on es van detectar els primers casos d'infecció massiva , els protagonistes van ser:

** BRAIN* un virus paquistanés a la Universitat de Delaware

** LEHIGH* a la Universitat del seu mateix nom

** DIVENDRES 13* a la Universitat hebrea de Jerusalem.

Els virus són sens dubte els programes danyosos per excel·lència, però existixen altres rutines que poden destrossar els sistemes dels PCs així tenim:

* Els cucs i conills: són programes que tenen la capacitat de reproducció igual que els virus, tenen per objectiu realitzar múltiples còpies de si mateix que sol acabar per desbordar i col·lapsar el sistema. El cuc més famós va ser el de *Robert Moriu* que va aconseguir bloquejar la xarxa ARPANET.

* Els cavalls de Troia o troians: són programes que es presenten en forma d'aplicació normal, però que en el seu interior posseïxen un codi destructiu, no tenen capacitat de replicació. Un dels més coneguts va ser la

SIDA.

* Bomba lògica: és un programa que s'executa al produir-se un fet determinat (una data, una combinació de tecles, etc.) si no es produïx la condició el programa roman ocult sense exercir cap acció, esta tècnica cap la seua utilització per programadors fraudulentament, per a així assegurar-se una assistència tècnica que només ells podran saber d'on ve i a més de forma periòdica.

* Els applests Java i active X:vénen de la mà dels llenguatges orientats Internet, que han permés la potenciació i flexibilitat de la xarxa, però també obrin un nou món a explotar pels creadors de virus.

FUNCIONAMENT

Els virus són simplement programes creats per persones amb un alt grau de coneixements sobre programació. El llenguatge més utilitzat en el seu desenrotllament és l'ensamblador per la seua potència encara que s'utilitzen tots: L'objectiu del virus consistix a replicar-se a si mateix de forma transparent l'usuari, dificultant així al màxim la seua detecció. Per a poder replicar-se necessita ser executat a l'ordinador, per la qual cosa recorre de manera habitual a unir-se a fitxers executables modificant-los o a situar-se en els sectors d'arrancada i taula de partició dels discos. Una vegada que s'executen solen quedar residents en la memòria a l'espera d'infectar a altres fitxers i discos.

Els virus residents intercepten els vectors d'interrupció, modificant la taula que conté , perquè apunten el seu codi. Els vectors són els encarregats de prestar els serveis al sistema; d'esta manera, quan una aplicació cride a un d'eixos serveis el control és cedit al virus. Amb el control del sistema, el virus es disposa a la reclinació, ja que una crida al servei d'execució o còpia d'un fitxer pot ser interceptada gràcies a les modificacions dels vectors d'interrupció i procedir a la seua infecció, el més usual per a això consistix a afegir el codi víric al final del fitxer i modificar la capçalera d'esta perquè apunte el virus. Al final del codi del virus hi haurà un nou bot al començament del programa original perquè s'execute amb normalitat i l'usuari no sospite.

Finalment el virus sol contindre un efecte que es farà visible en

determinades circumstàncies (una data , un número determinat d'infeccions, etc.) que faran despertar l'efecte, que pot variar des d'un innocent missatge que apareix en pantalla fins a la perduda total de la informació del nostre disc dur.

Els virus més avançats utilitzen tècniques per a fer més efectiu el seu treball així mitjançant la tècnica de:

Stealh: el virus amaga els signes visibles de la infecció que podrien delatar la seua presència

Tunneling: , intenten eludir els mòduls residents dels antivirus mitjançant punters directes als vectors d'interrupció (els mòduls residents dels antivirus funciona de forma assemblada els virus però amb propòsit totalment diferent).

Autoencrptació: permet que el virus sé encripte de manera diferent cada vegada que infecta un fitxer. D'esta forma dificulta la detecció dels antivirus. Normalment són detectats per la presència de la rutina de desencriptació ja que esta no diversa. La contramesura dels virus per a impedir ser detectats d'esta forma és varia el mètode d'encriptació de generació en generació és a dir , que entre distints exemplars del mateix virus no existixen coincidències ni tan sols en la part del virus que s'encarrega de la desencriptació; són els anomenats *polimorficos*

TIPUS DE VIRUS

DEPENENT DEL LLOC ON S'ALLOTGEN:

VIRUS DE BOOT: utilitzen el sector d'arrancada, el quin conté informació sobre el tipus de disc, número de pistes, sectors, cares, grandària de la FAT, sector de començament, etc. A tot això cal sumar-li un xicotet programa d'arrancada que verificà si el disc pot carregar el sistema operatiu. Els virus de BOOT utilitzen este sector d'arrancada per a ubicar-se, guardant el sector original en una altra part del disc: En moltes

ocasions el virus marca els sectors on guarda BOOT original com defectuosos; d'esta forma impedixen que siguen esborrats.

En el cas dels discos durs poden utilitzar també la taula de particions com a ubicació solen quedar residents en memòria al fer qualsevol operació en un disc infectat, a l´espera de replicar-se en altres , com a exemple tenim el BRAIN.

VIRUS DE FITXER: infecten arxius i tradicionalment els tipus executables COM i EXE han sigut els més afectats, encara que en estos moments són els fitxers de documents (DOC, XLS, SAM....) els que estan en voga gràcies als virus de macro. Normalment inserixen el codi del virus al principi o al final de l'arxiu, mantenint intacte el programa infectat. Quan s'executa, el virus pot fer-se resident en memòria i després torna el control al programa original perquè continue de mode normal: El divendres tretze és un exemple de virus d'este tipus.

DINS DELS VIRUS DE FITXERS:

* *VIRUS D'ACCIÓ DIRECTA*: són aquells que no queden residents en memòria i que es repliquen en el moment d'executar-se un fitxer infectat

* *VIRUS DE SOBREESCRIPTURA*:corrompen el fitxer on s'ubiquen al sobreescriure'l.

* *VIRUS DE COMPANYIA:* aprofita una característica del DOS, gràcies a la qual si cridem a un arxiu per a executar-lo sense indicar l'extensió del sistema operatiu buscara en primer lloc el tipus COM. Este tipus de virus no modifica el programa original, sinó que quan troba un fitxer EXE crea un altre d'igual nom contenint el virus amb extensió COM. De manera que quan teclegem el nom executarem en primer lloc el virus i posteriorment este passara el control a l'aplicació original.

* *VIRUS DE MACRO*: estan programats usant el llenguatge de macros *WordBasic*, gràcies al quin poden infectar i replicar-se a través dels fitxers ms-MS-Word (DOC). En l'actualitat s'han estés a altres aplicacions com Excel i a altres llenguatges de macros com és el cas dels fitxers SAM del processador de textos de Lotus. S'ha de destacar que són

multiplataforma quant a sistemes operatius ja que depenen únicament de l'aplicació. Un exemple d'este virus és el Concep que s'incorporà accidentalment en un CD de la companyia Microsoft.

** VIRUS BAT:* col·locant ordenes DOS en arxius de procés per lots aconseguixen replicar-se i efectuar efectes danyosos com qualsevol altre virus.

** VIRUS DE MIRC:* vénen a formar part de la nova generació Internet i demostren que la xarxa obri noves formes d'infecció. Consistix en un scrip per al client d'IRC mirc. Quan algú accedix a un canal d'IRC on es troba alguna persona infectada, rep per DCC un arxiu anomenat "scrip ini". Per defecte, el subdirectori on es descarreguen els fitxers és el mateix on esta instal·lat el programa, C:\MIRC. Açò causa que el "script. Ini" original siga sobreescrit pel nou fitxer maligne.

** NOU SCRIPT:* permet als autors i a qualsevol persona que conega el seu funcionament, des de desconnectar l'usuari infectat de l'IRC fins a accedir a la informació sensible del seu ordinador. Així, per exemple poden obrir-ne un FTP en la maquina de la víctima, accedir a l'arxiu de claus de Windows 95 o abaixar-se el "etc/password" al cas que siga Linux

VIRUS BENIGNE: una bona utilització de les tècniques que empren els virus poden reportar-nos beneficis i ser summament útils. Per exemple per a parchear sistemes a través d'extenses xarxes LAN. El programa s'infecta d'ordinador a ordinador modificant part d'un programa que causa fallades en el sistema, i una vegada solucionat l'error s'autodestruix.