

ELS VIRUS INFORMÀTICS. CONCEPTES GENERALS

Què és un virus informàtic?

Un virus informàtic és un programa d'ordinador que té, com a principal característica, la capacitat per **reproduir-se**, independentment de la voluntat de l'usuari.

A més de copiar-se a si mateixos, els virus tenen altres efectes sobre els ordinadors on han aconseguit instal·lar-se. Hi ha virus que tenen efectes nocius: esborrar informació del disc, fer malbé programes perquè no es puguin executar, etc. N'hi ha d'altres amb efectes que, bo i no ser destructius, molesten. Aquest seria el cas del virus que fa passejar una pilota per la pantalla.

Sovint els efectes no es noten immediatament després de la contaminació. Hi ha un **període d'inactivitat** que permet als virus encomanar-se als altres disquets i ordinadors abans de ser detectats.

Els virus, per activar-se i fer la seva feina, han de ficar-se a la memòria de l'ordinador (quedar residents). Des de la memòria interfereixen en el funcionament dels programes i es reproduïxen en tots els disquets que passen per l'ordinador o bé s'envien a través del correu electrònic

La forma de propagació dels virus està relacionada amb el lloc on viuen els virus (s'amaguen). Els virus es poden classificar en dos grans grups, segons el lloc on es col·loquen:

- els que s'amaguen als fitxers executables
- els que ho fan a les zones privilegiades del disc, la BOOT, la FAT...

Si un fitxer executable (acostuma a tenir extensió .EXE, .COM, .OVL o .SYS) ha estat contaminat per un virus i és executat, el virus s'activa i passa a la memòria de l'ordinador; des d'allí pot contaminar qualsevol altre programa executable que es posi al seu abast.

Els fitxers de dades (poden tenir extensions com .DOC, .TXT, .XLS, .WRI, ...) és molt poc probable que es contaminin ja que mai s'executen i, per tant, no serveixen per reproduir els virus.

Ultimament, però, hi ha virus en fitxers amb extensions .DOC que, tot i que són fitxers que contenen informació textual, contenen **macros**. (programes inclosos dins dels fitxers de dades, un cas típic són les macros de word o excel)

Alguns virus s'amaguen a zones privilegiades del disc, com són la taula de particions del disc dur (MBR), el sector d'arrencada (BOOT), la taula de localització de fitxers (FAT) o el directori arrel (C:/). Aquests virus passen del disquet al disc dur i a l'inrevés, independentment del tipus de programes o arxius que continguin. Una forma habitual de contaminació és engegar un ordinador amb un disquet infectat a la unitat A: Són virus per a despistats.

La propagació de virus mitjançant les comunicacions telemàtiques és cada vegada més freqüent i cal prendre mínimes mesures de seguretat: verifiqueu els fitxers que recupereu de la xarxa o que us enviïn per correu electrònic.



En termes generals el virus sempre són executats per l'usuari de manera no intencionada. Per tant els virus més destructius són els que es camuflen millor, generen reclams i donen confiança a l'usuari perquè l'executi i així poder instal·lar-se a l'ordinador.

Sistemes d'entrada dels virus a l'ordinador

Les possibles vies d'entrada són:

- **Unitats de disc removibles:** disquets, CD-ROM, Zip's o Jazz's
- **Intranets, xarxes d'ordinadors:** a través dels fitxers compartits a la xarxa o quan un ordinador no infectat es posa en contacte amb un ordinador infectat. En la transferència de informació dins de la intranet es poden transferir també fitxers que continguin virus.
- **Internet:** és el sistema més utilitzat per la propagació dels virus. Bàsicament pels següents camins:

Correu electrònic, en forma de fitxer adjunt

Pàgina web: En termes generals les pàgines web són fitxers de text i imatges associades. Ara bé una pàgina pot contenir controls ActiveX o applets de Java (petits programes) que si que poden contenir virus

Tipus de virus

Virus de fitxer:

Són la majoria i tenen extensions EXE o COM (executables), la seva execució és el que activa el virus. Tot i que poden existir virus en diferents característiques, segons la seva manera d'actuar el podem classificar en:

Virus residents: Es queden vigilants a la memòria principal. Quan executem qualsevol aplicació la infecten, afegint el seu propi codi al fitxer que hem executat.

Virus d'acció directa: Quan s'activa intenta crear còpies de si mateix. Normalment es situarà dins de l'AUTOEXEC.BAT. I cada cop que engeguem l'ordinador actuarà.

Virus de sobreescritura: rescric els fitxers que infecta i els deixa irrecuperables.

Virus company: Aprofita la particularitat de que el sistema executa primer el fitxer amb extensió COM, quan troba dos fitxers amb el mateix nom, però un amb extensió EXE i l'altre amb COM. Si prenem per exemple el Word (Windword.exe) el virus crearà una còpia amb el nom Windword.com. Quan executem el word el sistema executarà primer el virus i després transferirà el control al sistema perquè executi el correcte. L'usuari confiat no se'n adonarà fins que sigui massa tard.

Virus de Boot (Boot: sector d'arrencada del disc dur o del disquet on es guarda la informació sobre les característiques del disc). El virus actua quan arrenquem amb un



disquet o disc dur infectat, prenen el control del sistema operatiu. (cal evitar posar en marxa l'ordinador amb un disquet posat)

Virus macro: S'amaguen dins dels petits programes anomenats macros i que ens permeten automatitzar tasques amb el Word, Excel, Acces... S'executen quan l'usuari utilitza la macro i en general solen ser perillosos i de ràpida propagació.

Virus FAT (directori de localització de fitxers i carpetes): Cada fitxer o carpeta té una "adreça" dins del disc dur. Totes aquestes adreces són recollides a la FAT. El virus actua modificant aquesta adreça i col·locant-se en l'adreça d'altres programes. Per tant quan executem els programes el que realment fem és executar el virus. Tot i que pot exercir una gran capacitat de infecció, no sol anar més enllà de la FAT. Si executem un scandisk trobarem una gran quantitat d'errades que indicaran tot allò que el virus ha modificat.

On s'amaguem els virus?

- Memòria principal: És el virus resident, es col·loca a la RAM esperant que executem algun programa
- A les macros: És la manera de infectar fitxers no executables.
- A la BOOT (sector d'arrencada dels disquets) o a la Master BOOT (MBR, sector d'arrencada del disc dur o partició).
- Fitxers adjunt al correu electrònic
- A les pàgines web amb applets de Java o controls ActiveX

Com detectar si un ordinador està contaminat per un virus

Es pot notar que un ordinador està contaminat per un virus quan aquest comença a tenir un comportament diferent de l'habitual, presentant algun d'aquests símptomes:

- Es produeixen efectes visuals a la pantalla de l'ordinador: caràcters que es belluguen, una pilota botant, una zona que es desplaça, lletres a l'inrevés o que cauen, el disc dur funciona sense que hàgim fet res...
- Els programes funcionen més lentament del que és habitual.

És aconsellable una revisió periòdica i sistemàtica del disc dur de l'ordinador amb un detector de virus. És per tant una feina que cal introduir dins de les rutines habituals del Punt Òmnia

Cal tenir present que un mal funcionament del sistema no sempre és imputable a un virus: de vegades els ordinadors s'espantllen o alguns programes no funcionen adequadament. Un usuari poc experimentat pot no conèixer el funcionament correcte d'un programa i pensar que té virus.



La prevenció és la millor defensa contra els virus

La millor prevenció contra els virus és evitar la utilització en l'ordinador de disquets i programes de procedència dubtosa, disquets que no tinguin les mínimes garanties d'higiene. També cal vigilar els correus electrònics que contenen fitxers adjunts (sobre tot si són fitxers executables).

Malgrat aquest consell, sovint resulta indispensable instal·lar programes nous al disc dur, llegir disquets amb arxius de dades o desar les pròpies dades en disquets per tal de tenir-ne una còpia de seguretat. Abans de fer servir aquests disquets és molt recomanable efectuar una comprovació amb algun detector de virus. Aquest consell és aplicable a qualsevol disquet, sigui quin sigui el seu origen.

Protegir d'escriptura tots els disquets on no s'hagi d'escriure. D'aquesta manera es pot evitar que una contaminació afecti els disquets. Com a mínim, la desinfecció posterior serà més fàcil i les dades importants estaran protegides.

Fer còpies de seguretat de les dades i els programes tan sovint com calgui és una de les millors garanties contra els efectes nocius dels virus.