Atacs al programari

Quan en informàtica parlem de programari (*software*), ens estem referint als programes d'un ordinador. El maquinari (*hardware*) és la màquina en si. Avui dia hi ha programes que poden esborrar o alterar la informació d'un ordinador o altres programes. O sigui, hi ha atacs al programari no desitjats. No tots els atacs són virus. Fem-ne una classificació:

- Cavall de Troia: programa que en executar-se té una conseqüència maligna. Per exemple, un joc que esborri tot el disc dur en executar-lo.
- Bombes lògiques: programes que s'executen sota unes determinades circumstàncies (dia i hora concrets) i que són perjudicials.
- Cucs: programes perjudicials que podem trobar a la Xarxa.
- Virus: programes malignes amb la característica que es poden autocopiar.

Els virus. Introducció

La característica més important que té un programa anomenat virus és la capacitat d'autocopiar-se.

Hi ha molta desinformació sobre aquest tema. La gent pensa que si el seu ordinador és contaminat per un virus, això serà catastròfic. Aquesta idea no és certa del tot. Normalment, un virus no té una conseqüència catastròfica (n'hi ha alguns que sí, però són pocs), ja que si la tingués no es podria replicar a altres màquines. El detectaríem massa aviat i no donaria opció de rèplica.

Internet ha fet que els virus tinguin més importància, ja que avui dia són la major font de contaminació. Abans només ens podíem infectar si agafàvem un disquet que ja ho estigués. Ara, podem agafar un virus a través de la Xarxa.

El fet de l'existència dels virus ha fet que algunes empreses s'especialitzessin en la construcció de programes de detecció i eliminació d'aquests virus, els anomenats antivirus. Com que cada mes en surten molts (el setembre de 1999 s'estimava que hi havia cap a 2000 virus nous al mes), els programes antivirus necessiten actualitzacions contínues. En setembre de 1999 es coneixien al voltant de 45.000 virus diferents.

Una breu història

El 1984, el Dr. Cohen va fer una tesi doctoral sobre la possibilitat que els programes es reproduïssin. Així, l'any 1986 va néixer el primer virus amb cara i ulls: el Brain, construït pels germans Alví. El 1987 es va crear el primer antivirus. L'any 1992 és el del famós virus Michelangelo, que destrueix tot el disc dur. L'any 1995 va sorgir el primer virus de macro.

Classificació

Podríem fer moltíssimes classificacions de virus, però sembla lògic fer-ne una segons el lloc d'infecció. Així podem tenir:

- Virus sector d'arrancada: substitueixen la informació del *boot* (dimensions de la informació, adreces dels fitxers en el disc, etc.) i traslladen a una altra part del disc la informació bona. Es contagien arrancant des d'un disquet posat (que no té per què ser d'arrancada: només cal intentar arrancar amb un disquet contaminat, encara que aquest no sigui d'arrancada i veurem que, tot i que no arrancarem, sí que ens contaminarem igualment).
- Virus paràsits: escullen un fitxer i s'hi col·loquen. No se sap mai en quina part del fitxer escollit es col·locaran. La forma de contagi és l'execució de programes contaminats.
- Virus de macro: fan servir els programes de macro (Word, Access, etc.). Obrint un document infectat s'infecta la plantilla, i a partir d'aquí qualsevol cosa que fem amb aquesta plantilla quedarà infectada.
- Virus multipartits: infecten el sector d'arrancada i a més alguns programes.
- Virus companys: infecten els fitxers d'extensió COM i EXE, o sigui els programes executables.
- Virus de vincle: modifiquen els *clusters* on s'ubiquen els programes, de manera que els *clusters* apuntin al virus i aquest cridi els programes.

Els virus a Internet

A Internet es mou molta informació; per tant, s'hi mouen molts virus. Abans es podia aïllar un virus fàcilment. Ara, amb Internet, s'escampen amb molta més facilitat. N'hi ha que estan específicament creats per a la seva replicació a Internet (Happy99, Melisa, Monopoly, etc.).

El 90% d'infeccions a Internet són degudes als annexos als missatges electrònics, i el 10% restant a descàrregues de programes de la Xarxa (FTP). Avui dia, el fet d'obrir i llegir un missatge no té cap risc; el risc està en els annexos que arriben amb alguns.

Un exemple és el virus Melisa, que va tenir molta popularitat ja que es propagava molt fàcilment. El Melisa funciona de la forma següent: l'usuari rep un missatge en anglès al seu nom i, com a assumpte important, acompanyat d'un document Word amb adreces pornogràfiques. Quan l'usuari obre