

ELS PROGRAMES ANTIVIRUS I ANTISPYWARES

Virus i antivirus

Tot i que els virus no són l'única amenaça per al bon funcionament del nostre ordinador, actualment la seva proliferació ha fet que siguin un perill seriós, ja que es transmeten molt fàcilment a través d'internet i el correu electrònic, que són dos dels elements informàtics més utilitzats. Per aquest motiu, avui en dia és pràcticament imprescindible disposar d'un programa que ens protegeixi d'aquest problema o ens netegi l'ordinador si calgués.

Un virus informàtic no és res més que un programa amb finalitats malignes que, a més a més de espiar l'usuari o provocar-li problemes, es reproduïx automàticament. Aquests mecanismes d'autoreproducció és el que fa que els virus siguin tan perillosos ja que una màquina infectada pot propagar còpies del virus i infectar altres sistemes. Aquesta és justament la intenció del virus. Generalment un virus no afecta un ordinador en general, sinó parts d'aquest, com per exemple el programari o la informació emmagatzemada al disc dur, per la qual cosa pot continuar funcionant però amb molts defectes.

Les vies d'entrada dels virus als ordinadors són diverses, però les principals són Internet (les pàgines actualment ja poden ser hostes de virus informàtics), els disquets i d'altres removibles (cd's, llapisos...) i, sobretot, el correu electrònic que actualment és el principal propagador d'infeccions. Un cop l'ordinador es troba infectat per un virus es probable que l'usuari tardi en adonar-se'n, ja que una de les principals virtuts dels enemics dels ordinadors és que passen desapercebuts, a no ser que tinguin objectius tan malignes com esborrar informació. La memòria RAM de les màquines i els fitxers que contenen macros són els principals amagatalls dels virus. Per si això fos poc, els programadors de codis maliciosos disposen d'eines suficients per fer que aquests programes passin desapercebuts pels propis antivirus, per la qual cosa estem parlant d'una constant lluita entre virus i antivirus per ser detectats i passar desapercebuts. Així doncs, un dels elements principals de la lluita contra els virus és l'actualització. A causa de la gran proliferació dels virus ja no n'hi ha prou amb tenir un programa que els aturi sinó que cal que el tinguem contínuament al dia per evitar que els virus més nous entrin a la nostra màquina burlant un programa antiquat. Actualment l'actualització, més enllà del fet que apareixen nous virus cada dia, no suposa un handicap massa gran en tant que el procés d'actualització es pot fer per internet i tots els programes

antivirus disposen d'una aplicació especial (Up-date) que en té cura sense que l'usuari hagi de fer res, excepte, això sí, connectar l'ordinador a la xarxa i deixar-lo fer.

Malgrat tot, però, si l'usuari no és curós amb el seu correu, les pàgines que visita i l'actualització de l'antivirus, és possible que algun d'aquests programes malignes entri al seu ordinador. No hi ha una simptomatologia clara per endevinar si a pesar dels esforços ens han burlat, però si es detecta una lentitud poc habitual en la nostra màquina, si l'ordinador es bloqueja sovint i necessitem reiniciar-lo, si s'apaga sobtadament, si es tanquen programes, si es connecta a internet sense una ordre expressa nostra o si no podem accedir a alguns fitxers a causa d'errors o perquè han desaparegut pot ser (atenció que això no vol dir que sempre) que ens trobem davant un virus. En aquest cas, cal que utilitzem el nostre programa antivirus, ben actualitzat, per intentar eliminar-lo. A vegades el programa detecta el virus però no el pot esborrar. En aquest cas podem recórrer a les pàgines web del nostre proveïdor d'antivirus que sol donar informació de com esborra virus concrets. Tanmateix, hem de tenir en compte que un cop esborrat el virus aquest ens pot haver fet malbé alguns fitxers del nostre ordinador o, senzillament, podria ser que, malgrat tot, no ens en poguéssim desfer. En aquest cas caldrà demanar ajut especialitzat als tècnics informàtics que esborraran el virus, restauraran els fitxers afectats i, en molts casos, hauran de tornar a instal·lar alguns programes al nostre ordinador.

De virus n'hi ha de molt diversos. De forma general podem dir que actuen sobre el sistema segons la seva tipologia. El virus tradicional es reproduïx infectant altres fitxers i danyant-los, ja que insereix el seu codi en ells, i entorpeix el funcionament general de la màquina recarregant-li la memòria. Però, ja des de fa força temps, existeix una tipologia de virus molt perillosa que s'anomenen Cucs o Trojans. Aquests entren a l'ordinador en forma de programa inofensiu (per burlar l'antivirus), però un cop dins l'ordinador s'executen i instal·len un altre programa maligne que es reproduirà a gran velocitat dins l'ordinador provocant nombrosos danys i fent que sigui molt difícil d'esborrar i de reparar-ne les malifetes, al mateix temps que envien informació sobre l'usuari a la seva pàgina d'internet. Per això cal anar amb molt de compte quan rebem o ens descarreguem fitxers executables d'internet.

Alguns dels virus més "famosos" que hi hagut són els següents (alguns encara estan actius...):

- **Core war:** és el precursor dels virus. Fou creat el 1949. Executava programes que disminuïen la memòria de l'ordinador.

- **I love you:** cuc que es propaga a través del correu electrònic i el xat. Es reenvia a través dels contactes de la nostra llibreta d'adreces. És molt destructiu.
- **Mydoom:** arriba per correu electrònic, en arxius adjunt, o en missatges d'error d'enviament de correus. Es propaga ràpidament i causa moltes destrosses.
- **Explore Zip:** trojà summament destructiu, fins al punt que l'FBI investiga qui és el seu autor. No té una manera fixa de penetrar.
- **Bagle.BC:** cuc que obre ports i compromet la confidencialitat de l'usuari. És perillós i deixa l'ordinador vulnerable davant altres infeccions.
- **Netsky.P:** Actualment actiu i molt perillós. Es distribueix per correu electrònic només en visualitzar-lo.
- **Fizzer:** virus extremadament perillós que captura les pulsacions de l'usuari per obtenir contrasenyes i dades confidencials.
- Per a qualsevol altre virus consulteu les pàgines dels proveïdors de programes antivirus.

Tot això ens planteja la pregunta de quin és el benefici que suposa crear un virus destructiu? Aquesta pregunta és de difícil resposta ja que, probablement, ningú disposa de tota la informació necessària per respondre-la. Tanmateix sembla ser que molts dels virus actuals han estat creats per aconseguir notorietat entre els enginyers informàtics. Els creadors de codis maliciosos solen pertànyer a petites cibercomunitats on la destresa per crear programes representa la millor virtut. Això ha arribat a tal punt que actualment és té notícia de lluites entre creadors de virus per veure qui infecta més ordinadors. Aquesta informació s'ha descobert mitjançant alguns missatges continguts en els mateixos virus i que insulten els seu contrincant. Una lluita així va ser protagonitzada entre els virus Netsky i Bagle, en què cada nova versió que sorgia anul·lava i substituïa la del contrincant.

Alguns programes antivirus que us poden interessar:

- Avira Antivirus (versió gratuïta i de pagament)
- Avast (antivirus gratuït)
- AVG (antivirus gratuït)
- Microsoft Security Essentials (antivirus i antispies gratuït)
- Kaspersky.
- McAfee, Norton i Panda: són bons antivirus però relantitzen molt el sistema (consumeixen molts recursos) i a més són cars.

A sota podeu veure la imatge del panell inicial de l'Antivirus Avira. Bàsicament ens informa de si tots els serveis estan activats, de quan s'ha realitzat l'últim anàlisi, si l'antivirus està actualitzat i de quan caduca la llicència. Fer exploracions periòdiques (cada mes com a mínim) és molt recomanable.



Spywares i adwares

L'últim estadi d'aquesta lluita contra les infeccions és l'aparició a internet dels spywares i adwares, és a dir programes o robots espia que capturen i envien informació sobre els nostre ordinador, que pot ser des de hàbits de navegació fins a contrasenyes. Aquests programes, que actualment són molt problemàtics, fan que la nostra navegació es vegi interferida i se'ns redirigeixi a les pàgines que a aquests programes els interessa, o bé que se'ns obrin contínuament pop-ups o pàgines de propaganda no desitjada, problema que té la seva extensió en el correu brossa o spam que rebrem contínuament al nostre correu electrònic, tot i que aquest, igual que els pop-ups segurament els patirem tot i no tenir cap d'aquests espies al nostre ordinador, ja que són les principals molèsties benignes que actualment trobarem en utilitzar internet. Per a aquest problemes tenim diferents solucions. Actualment les cases de programes antivirus venen un paquets de programes anomenats antimalware (software maliciós) que no lluiten només contra els virus sinó també contra totes aquestes altres amenaces. D'altres solucions són les barres d'eines que proveeixen firmes com Google, Yahoo o msn que ens bloquejaran els pop-ups sempre i quan el nostre ordinador no estigui infectat. Per lluitar contra els programes espia també podem descarregar-nos alguns programes anti-adware disponibles de forma gratuïta a internet o comprar-ne algun a la nostra botiga d'informàtica o descarregar-lo per internet. Actualment entre els més fiables s'hi compten el programa Ad-Aware Se Personal de la firma Lavasoft (descarregable de forma gratuïta a internet) i el programa Spybot-Search and destroy (també descarregable de forma gratuïta a internet). Si escollim descarregar altres programes antiespies d'internet cal anar amb compte ja que sota la seva aparença s'amaguen precisament alguns virus.

Si patiu algun dels símptomes següents és el moment de buscar l'ajuda d'alguns d'aquest programes: connexió a internet més lenta de l'usual amb gran nombre de pop-ups estranys, barres d'eines que no heu instal·lat i que no podeu treure, accessos directes (a l'escriptori, al menú inici, o a la barra d'inici ràpid) que no heu instal·lat i que reapareixen tot i que els esborreu, una pàgina d'inici del navegador que no desitgeu i que no podeu canviar, enllaços dins els menús o dins el menú de *Favoritos* o fins i tot trucades a un proveïdor d'internet que no és el vostre amb una tarifa molt diferent. Tingueu en compte que aquests programes espia us podeu causar tants o més problemes que els mateixos virus, per la qual cosa cal actuar ràpidament quan sospitem que en tenim algun dins el nostre ordinador. Actualment

és una de les plagues més freqüents entre els ordinadors que habitualment circulen per internet. La següent imatge reproduïx el funcionament d'un d'aquests programes.

Windows ja porta el seu propi AntiSpyware, el **Windows Defender**, tot i que se li escapen forces coses. Per això, si el nostre antivirus no en porta un d'incorporat, és bo fer-se amb un altra programa antispyware. Un dels més utilitzats (i a sobre és gratuït) és l'**Spybot Search & Destroy**.

La base d'aquest programa (i de tots) és tenir-lo actualitzat (**Cerca actualitzacions**). Un cop actualitzat, cal **Immunitzar** l'equip, o sigui, prevenir-lo de les amenaces conegudes (això s'ha de fer sempre després d'actualitzar). Finalment, cal fer anàlisis (com a mínim setmanals) de tot el sistema (**Cercar incidències**). Penseu que el sol fet de navegar per internet durant uns moments ens pot infectar ràpidament d'espies l'ordinador.



Spam o correu massiu

Finalment, pel que a l'Spam o correu brossa, en general els proveïdors de correu electrònic ja posen a les bústies eines per detectar-los i els aïllen en una carpeta especial que només haureu de tenir cura d'anar buidant. Si això no fos així, també hi ha disponible en el mercat programes anti-spam, per exemple per usuaris del programa Outlook. Generalment, aquesta propaganda no porta més problemes que la propaganda ordinària en paper, ens omple la bústia, però en un entorn tant canviant mai se sap.....