

# UF5-Manteniment d'equips microinformàtics.

## *NF1-Manteniment d'equips microinformàtics.*

NF1.1 Manteniment del maquinari.

NF1.2 Salvaguarda i recuperació de la informació.

**>> NF1.3 Malware: Virus i altres amenaces de seguretat.**

# Introducció al Malware

- Amb la proliferació de les xarxes informàtiques i del correu electrònic, l'ús de dispositius d'emmagatzematge portàtil i xarxes inalàmbriques han augmentat les amenaces i atacs a la seguretat de que podem ser objectes.
- Ara parlem de virus, hoaxes, phishing, mailbombing, hacking, spam, troians, cucs, spyware, adware, atacs DOS, sniffers, pharming, bots, botnets, ... segons la forma com actuen. A totes aquestes amenaces se'ls anomena de forma general com a: **MALWARE**

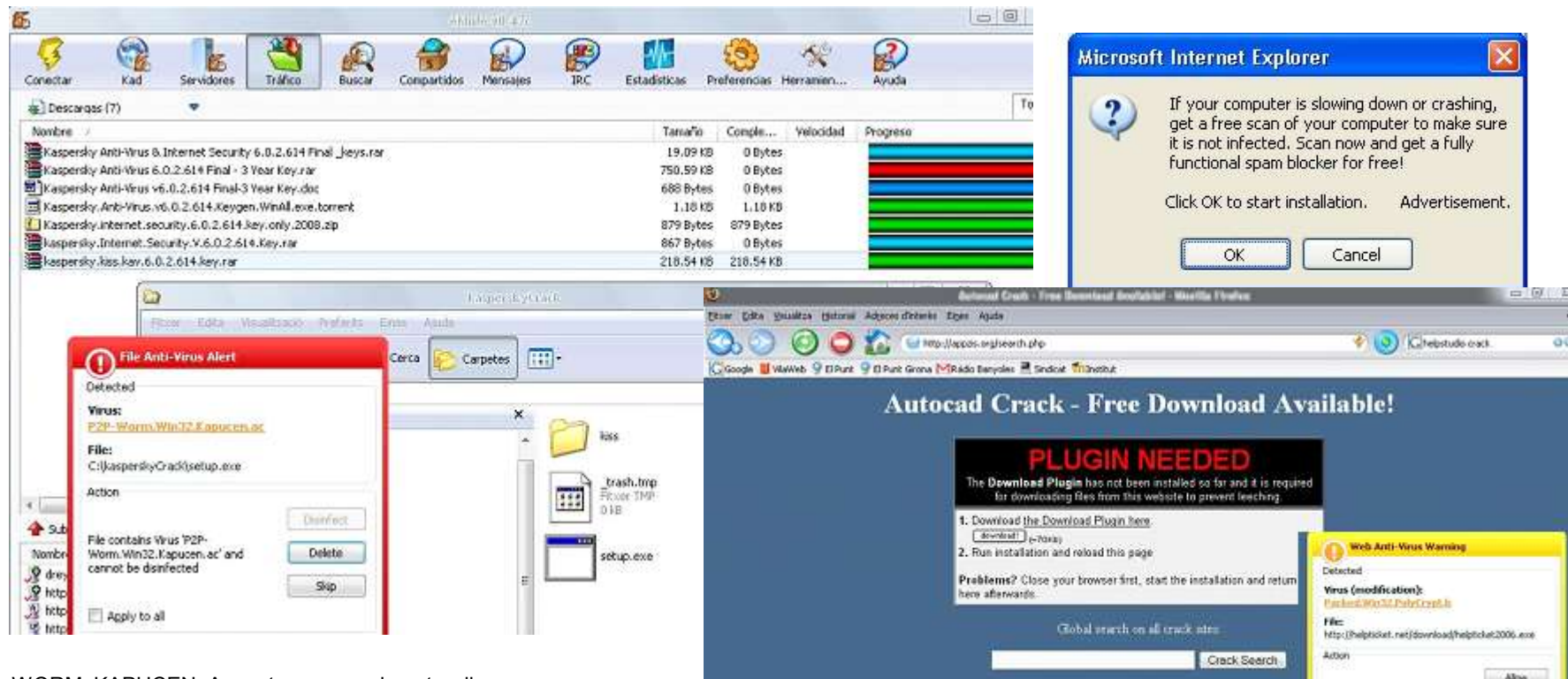
# Virus

- Un **virus informàtic** és un programa que té per objectiu alterar el funcionament normal de l'ordinador, sense permís o coneixement de l'usuari.
- Són programes que es poden replicar i executar per sí mateixos.
- Normalment, substitueixen fitxers executables per altres d'infectats amb el codi del virus.
- Els virus poden destruir de forma intencionada les dades emmagatzemades en un ordinador, tot i que també n'hi ha d'altres menys destructius que l'únic que fan és molestar o aprofitar els recursos atacats per realitzar activitats il·ícites sense coneixement de l'usuari.

## Funcionament d'un virus

- S'executa un programa que està infectat, sense que l'usuari se n'adoni.
- El codi del virus queda resident a la memòria RAM de l'ordinador, fins i tot quan el programa infectat amb el codi del virus ha acabat.
- El virus agafa el control dels serveis bàsics del SO infectant fitxers executables que es vagin executant.
- Finalment, es grava el codi del virus a d'altres programes, infectant-los, i creant així més rèpliques del virus.

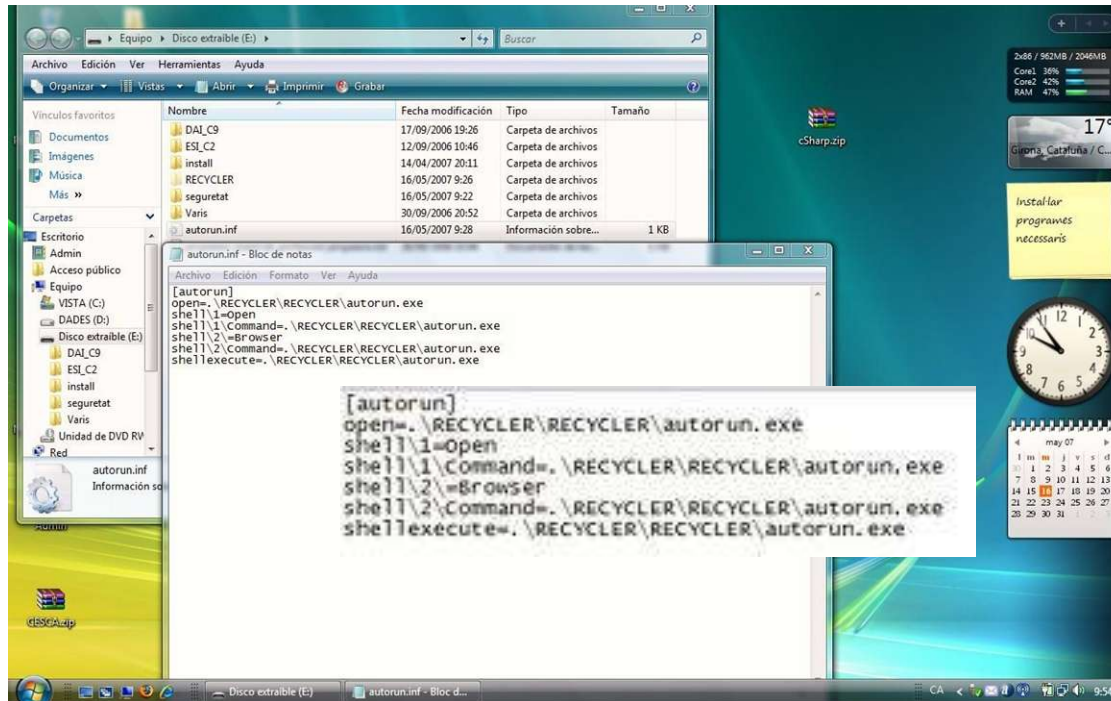
# Exemples de virus



**WORM\_KAPUCEN:** Aquest cuc normalment arriba en un sistema amb un arxiu descarregat des d'aplicacions peer-to-peer (P2P). Busca unes quantes carpetes de P2P, i es copia a si mateix utilitzant un nom d'arxiu específic, RAR o arxiu .ZIP per poder-se propagar fàcilment. També crea un arxiu de .TXT, que conté informació.

**Packed.Win32.PolyCrypt.b:** Aquest backdoor normalment arriba com un arxiu baixat per malware o bé forma ignorada per un usuari en visitar llocs web delictius. Obre un port a l'atzar i actua com servidor proxy. Escolta connexions remotes. Una vegada que s'estableix una connexió, escolta comandes que arriben d'un usuari delictiu remot, compromentent la seguretat de xarxa. També envia l'adreça d'IP del sistema afectat i el port a què s'obre a l'usuari remot. A més, impossibilita l'arranc del Comprovador d'Arxius del Sistema de Windows, que comprova i restaura arxius de sistema modificats.

# Exemples de virus



## Exemple de propagació per pendrive



Fitxer:

G:\RECYCLER\RECYCLER\autorun.exe

Programa troià

Backdoor.Win32.PcClient.wi ->

Backdoor o porta de darrera que amb funcionalitats de rootkit (accés com administrador des de l'exterior) amaga processos, fitxers i dades del registre; també roba informació sensible de l'ordinador infectat. Permet a un atacant remot realitzar accions arbitràries en la màquina infectada.

L'atacant pot entre d'altres coses

- \* Obrir un shell. Obrir i tancar la safata lectora de CD. Accedir a la informació guardada pel propi troià (títol finestres i dades entrades pel teclat). Descarregar, pujar a Internet i executar arxius. Enviar correu electrònic. Obtenir informació de la xarxa. Obtenir informació del sistema. Obre dos ports quedant a l'espera de les ordres de l'atacant.

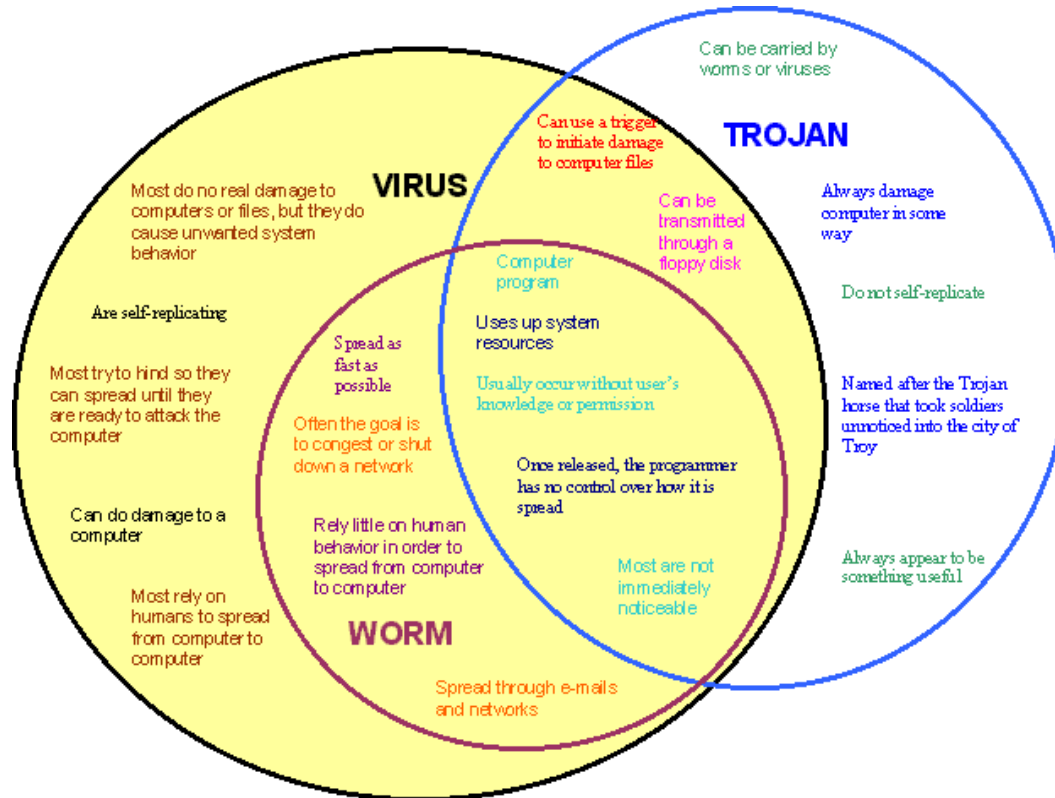


# Classificació dels virus

- Segons el que infecten

- 1<sup>a</sup> classificació.
  - *Virus que infecten fitxers.*
    - *Virus d'acció directa.*
      - » En el moment en que s'executen, infecten altres programes.
    - *Virus residents.*
      - » Quan s'executen, s'instal·len a la memòria de l'ordinador.
      - » Infecten als altres programes a mida que s'hi accedeix.
  - *Els que infecten el sector d'arrancada, (virus de boot).*
- 2<sup>a</sup> classificació.
  - *Virus de fitxers*, que modifiquen fitxers o les entrades de directori que indiquen el lloc on es guarden els directoris o fitxers.
  - *Virus de sistema operatiu*, que infecten fitxers del SO.
- 3<sup>a</sup> classificació. Per unificar la forma d'anomenar els virus.
  - Es fa referència a la plataforma on actua el virus i a algunes característiques importants (Classificació proposada per Computer AntiVirus Researcher Organization - CARO) però pot variar de fabricant d'antivirus a fabricant.
  - El prefix indica la plataforma que ataca W32 (Windows95, 98, 2000, 2003, XP, Me, NT 4.0, Vista,...) o bé Troj (Trojà) , I-Worm (Cuc d'Internet), OM (Macro de MSOffice)
  - @mm indica que té capacitat de *mass mailing* (enviament massiu de correu electrònic infectat). Si porta @m és propaga per correu però menys massiu, @dl vol dir downloader.
    - Exemple: el **W32/Hybris.A@mm** és un virus Hybris que es troba la plataforma win32, en la seva variant A (primera) i s'extén per enviament de correu massiu,

# Classificació dels virus





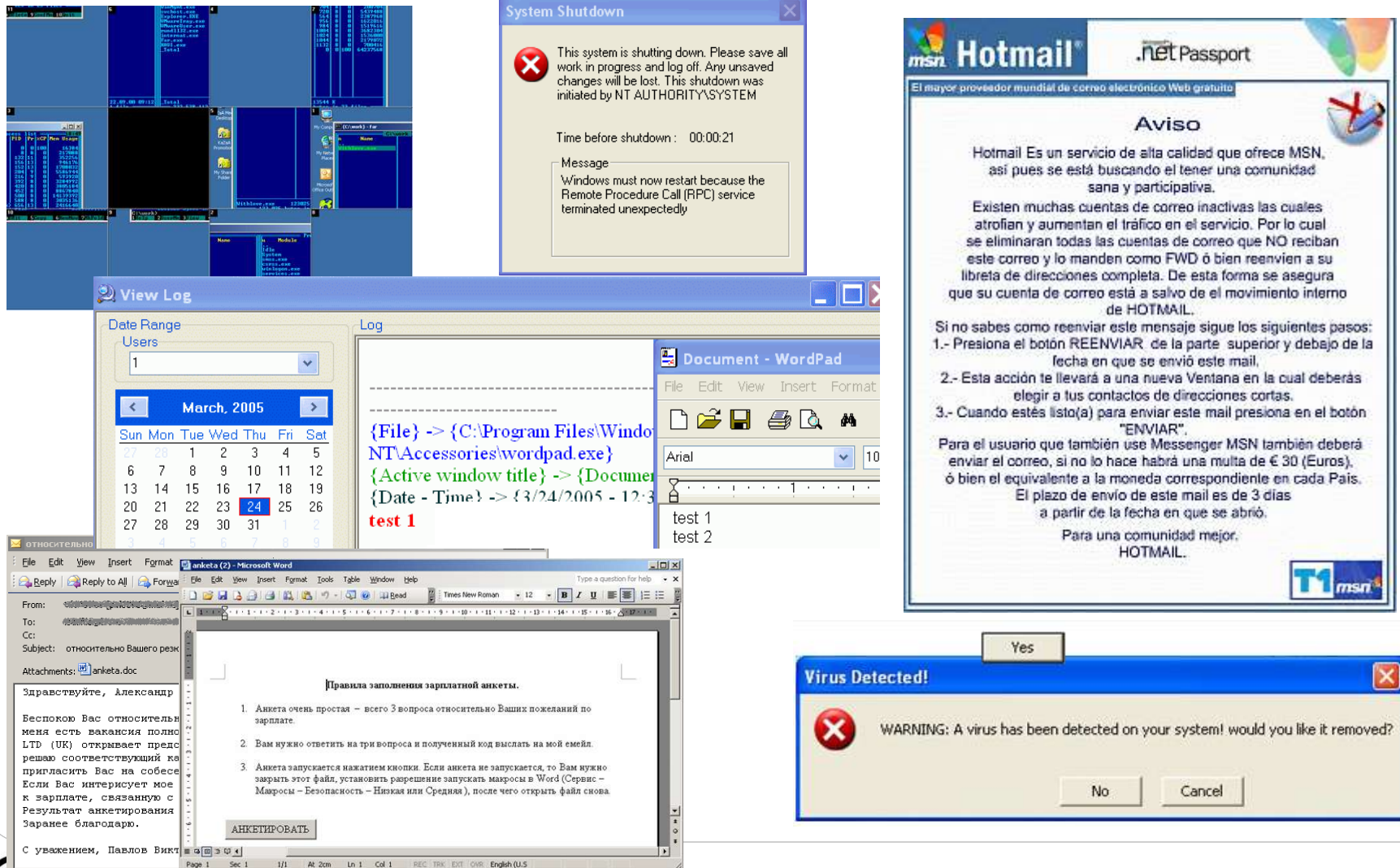
# Classificació dels virus

- **Tipus de virus**

- *Worms* o cucs
  - S'executen quan inicia el sistema operatiu, ocupant memòria i alentint l'ordinador
  - No infecten altres fitxers executables.
  - Utilitzen medis massius com el correu electrònic per propagar-se.
- Troians
  - Solen ser els més perillosos.
  - Funcionen igual que el cavall de troia: ajuden a l'atacant a entrar al sistema infectat, fent-se passar per continguts coneguts (salvapantalles, jocs, música, etc.).
  - De vegades descarreguen altres virus per fer més mal a l'equip.
- *Jokes* o virus broma
  - Virus que creen missatges de broma a la pantalla.
  - Poden executar el lector de CD/DVD obrint-lo i tancant-lo, controlar el mouse o el teclat, però sense fer cap mal.
- Hoaxes o virus falsos
  - Missatges amb informació falsa, que normalment s'envien amb correu electrònic, de vegades amb la finalitat de provocar confusió entre la gent que rep aquest tipus de missatge o de vegades perjudicant a algú o atacar l'ordinador amb enginyeria social (missatges com *borre este archivo del equipo* és un virus molt potent pels inexperts, ja que fan eliminar fitxers del sistema).
- Virus de macro
  - S'oculten en documents per poder-se propagar.
  - Utilitzen el llenguatge de programació VisualBasic per infectar fitxers Word, Excel, etc.
  - Són relativament fàcils de crear.

<http://www.viruslist.com/sp/virusesdescribed>

# Classificació dels virus



# Propagació de virus

## Worm Propagation

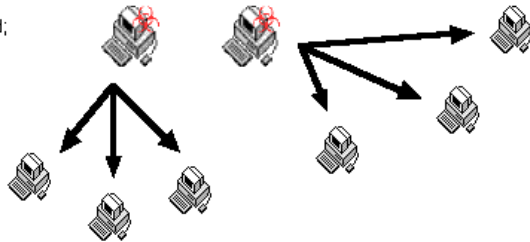
Step 1:  
Infected system sends packet to exploit RPC vulnerability to remote system.



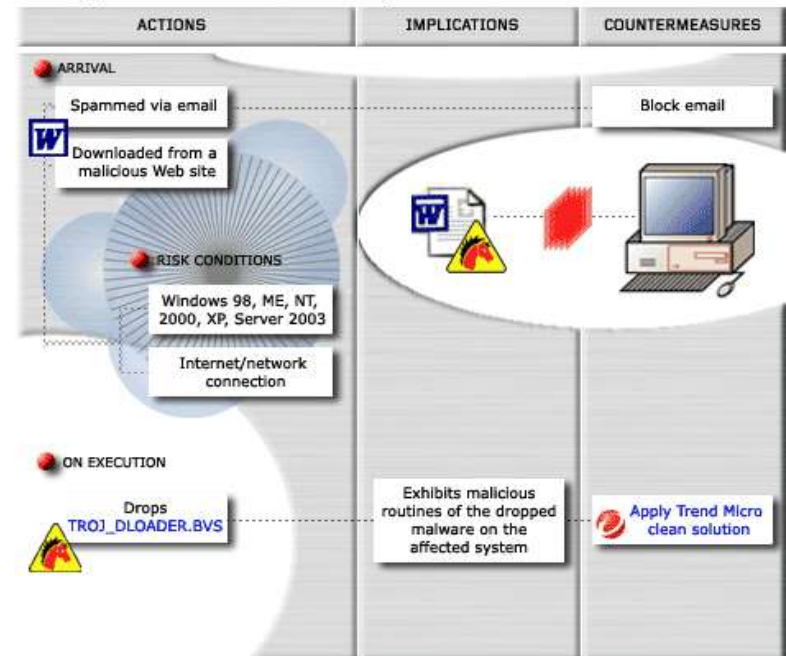
Step 2:  
If system is vulnerable, the RPC exploit causes it to open a connection back to the infected system to download a copy of the virus.



Step 3:  
Vulnerable system is now infected; both infected systems search for new vulnerable systems to infect. Process repeats as new unpatched systems are found.



## W97M\_DLOADER.BVS Behavior Diagram



## Síntomes d'infecció

- Programes que funcionen més lents del normal
- Augment de la mida en els fitxers, sobretot en els executables.
- Aparició de fitxers o processos “estranyys”
- Disminució de la RAM accessible per treballar.
- Sons o vídeos amb efectes estranyys

# Com treure un virus de l'ordinador?

- Utilitzant una eina antivirus
- Coneixent “el mal” que fa el virus
  - Hi ha webs que contenen molta informació sobre els virus més perillosos.  
<http://www.trendmicro.com/vinfo/virusencyclo/default.asp>
  - [www.alerta-antivirus.es](http://www.alerta-antivirus.es)
    - En aquesta web en castellà es pot cercar un virus i ens dona informació sobre el “mal” que provoca i la seva solució.



# Com treure un virus de l'ordinador?



The screenshot shows a Mozilla Firefox browser window displaying the 'Alerta-Antivirus.es: Detalles del virus Blaster.T' page. The browser's address bar shows the URL 'http://alerta-antivirus.red.es/virus/detalle\_virus.html?cod=3812'. The website has a red header with the title 'Alerta-Antivirus' and a subtitle 'Centro de Alerta Temprana sobre Virus y Seguridad Informática'. Navigation links include 'Acceso fácil', 'Mapa del Sitio', and 'RSS'. A search bar with the text 'Buscar' is visible. The main content area features a red banner for 'Blaster.T (Peligrosidad: 3 - Media)'. Below this, the text describes a new variant of the Blaster worm that exploits the RPC-DCOM vulnerability in Windows 2000/XP using port TCP 135. It mentions that this variant sends 'distintos' (different) packets. A 'Solución' (Solution) section follows, stating that Microsoft has published recommendations for protection. The first recommendation is to use the System Restore feature if the infection occurred on Windows Me or XP. The text also advises temporarily disabling System Restore if the virus cannot be removed by other means.

**Alerta-Antivirus**  
Centro de Alerta Temprana sobre Virus y Seguridad Informática

**Blaster.T (Peligrosidad: 3 - Media)**

Nueva variante del celeberrimo gusano Blaster, que explota la vulnerabilidad RPC-DCOM de Windows 2000/XP usando el puerto TCP 135.

Esta variante envía paquetes **distintos** para explotar la vulnerabilidad en sistemas Windows XP y Windows 2000, y tiene capacidad de puerta trasera.

**Solución**

Microsoft ha publicado una página con recomendaciones para protegerse del gusano Blaster y similares

1. Si utiliza Windows Me o XP, y sabe cuándo se produjo la infección, puede usar la característica de Restauración del Sistema para eliminar el virus volviendo a un punto de restauración anterior a la infección. (Tenga en cuenta que se desharán los cambios de configuración de Windows y se eliminarán todos los archivos ejecutables que haya creado o descargado desde la fecha del punto de restauración)

Si esto no es posible o no funciona es recomendable desactivar temporalmente la Restauración del Sistema antes de eliminar el virus por otros medios, ya que podría haberse creado una copia de seguridad del virus. Si necesita ayuda vea Deshabilitar restauración del sistema en Windows XP y Windows Me

## Eines: Antivirus

- Programes que tenen per funció la detecció i eliminació de virus informàtics i altres programes maliciosos (*malware*)
- Actualment hi ha molts antivirus al mercat: Panda, McAfee, Norton, Kaspersky, Avast, AVG, Clam, etc.
- Hi ha eines per eliminació de virus online
- És aconsellable utilitzar un disc d'inici amb un sistema lliure de virus, que incorpori un antivirus que permeti l'actualització per poder detectar i eliminar de forma fiable els virus (p.e. Linux Trinity amb antivirus Clam actualitzable i accés a NTFS).



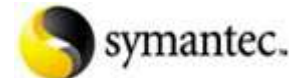
# Eines: Antivirus

- Tasques:
  - Detecció de virus en el *boot* abans de carregar-se completament el SO
  - Detecció de virus en els fitxers que es volen obrir.
    - Es fa abans de que el fitxer es carregui a memòria.
  - Detecció de virus dels fitxers durant el procés d'instal·lació de programari.
  - Detecció de virus en fitxers d'Internet i correu electrònic.
  - Escaneig complet del disc.
  - Posada en quarentena de fitxers, per tal que no es propaguin els virus.
  - Recuperació del SO que es trobi molt infectat, sense poder engegar.

# Eines: Antivirus

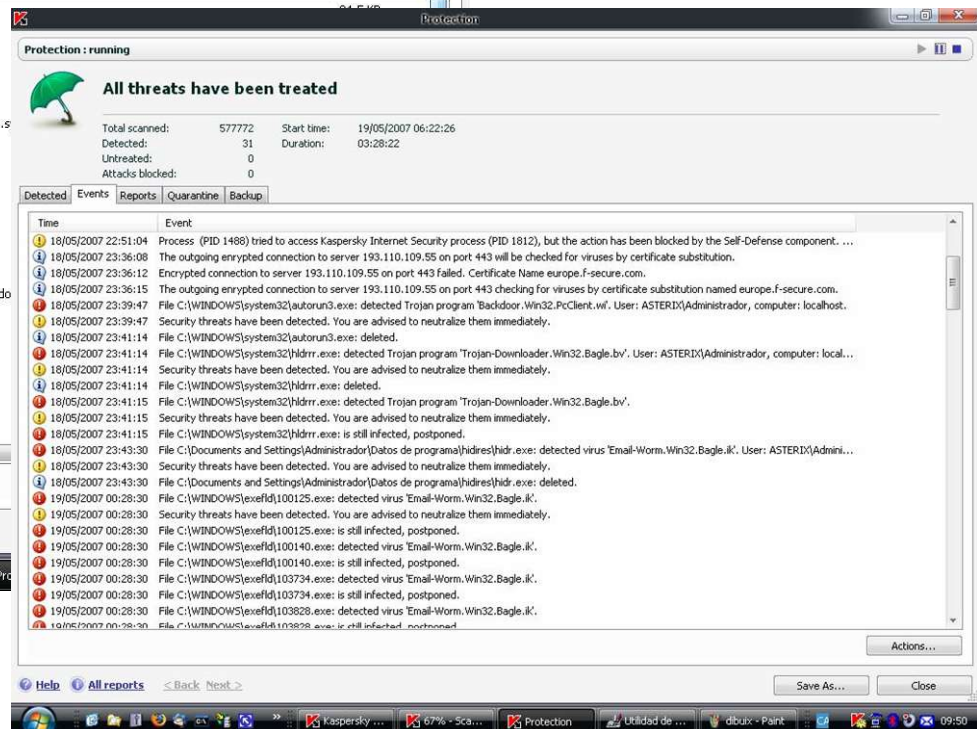
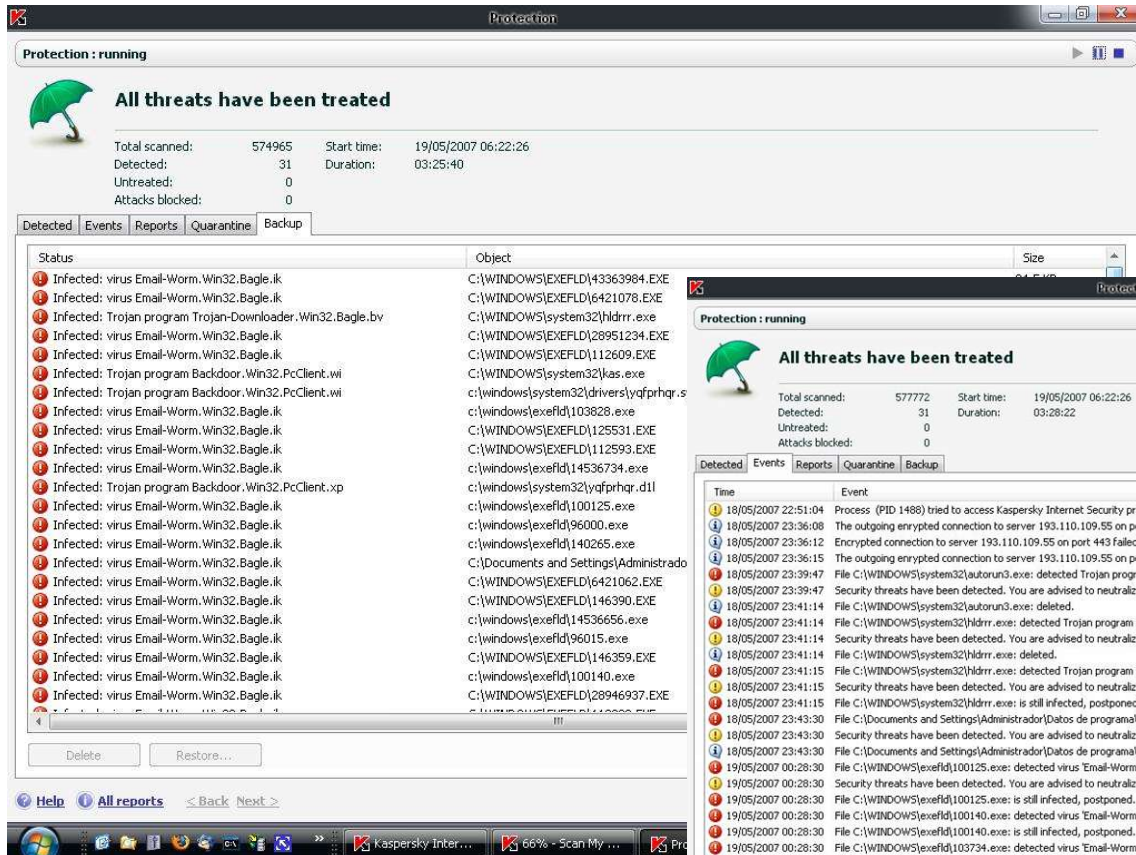
- Quan troba un virus, l'antivirus fa les següents accions:
  - Preguntar a l'usuari que vol fer amb el fitxer infectat
    - L'usuari escollirà entre desinfectar, aïllar, renombrar o esborrar el fitxer.
      - Desinfectar
        - » Sempre que sigui possible, intentarà desinfectar els fitxers
      - Aïllar
        - » S'aïllen temporalment els arxius conflictius sense esborrar-los
      - Renombrar els fitxers
        - » Podem renombrar si no es pot fer la desinfecció perquè el virus ha fet malbé el fitxer.
      - Esborrar els fitxers
        - » Ho decideix l'usuari.
        - » Quan no es pot desinfectar el virus que porten els fitxers.
      - Només informar

# Eines: Antivirus



# Eines: Antivirus

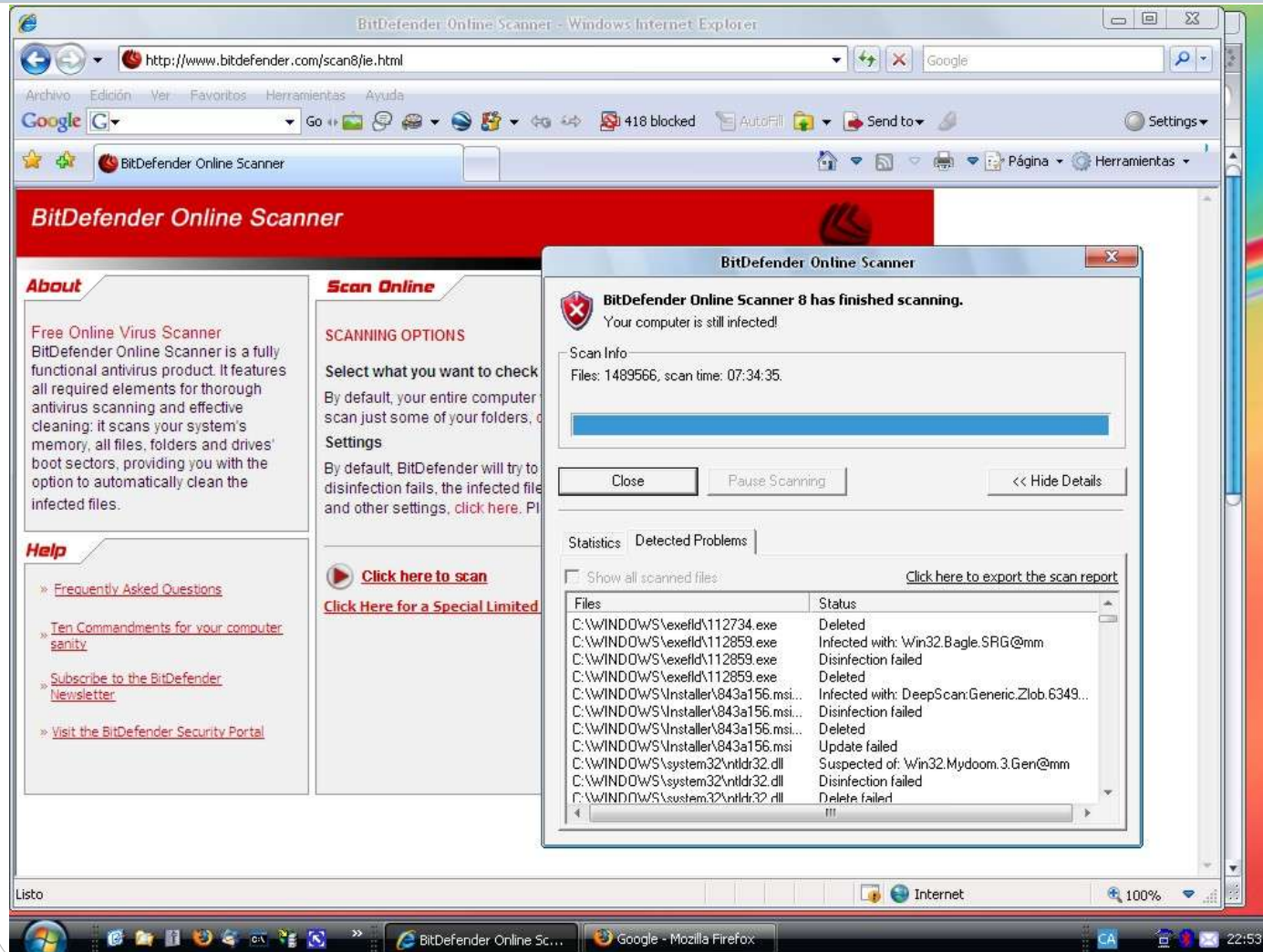
Antivirus  
local



# Eines: Antivirus



# Eines: Antivirus

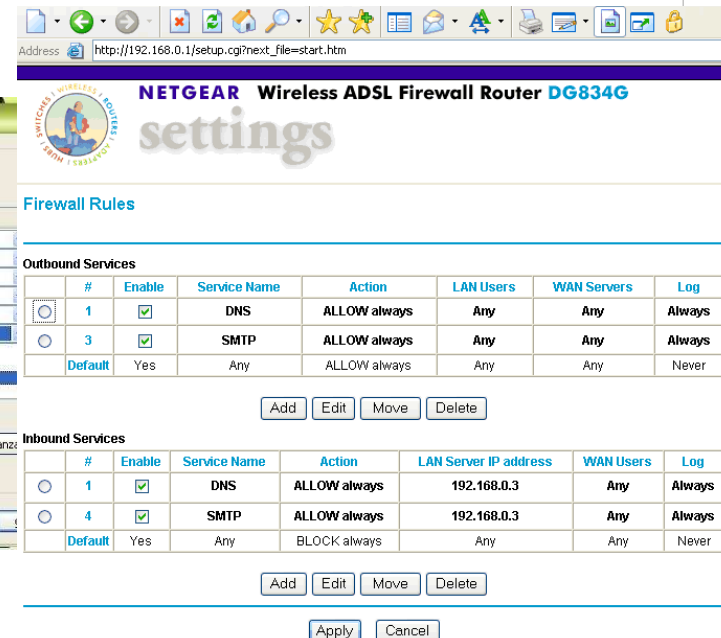
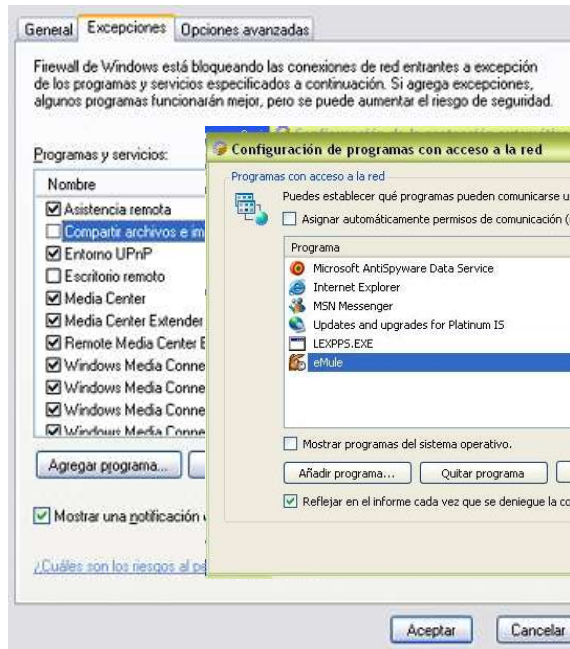
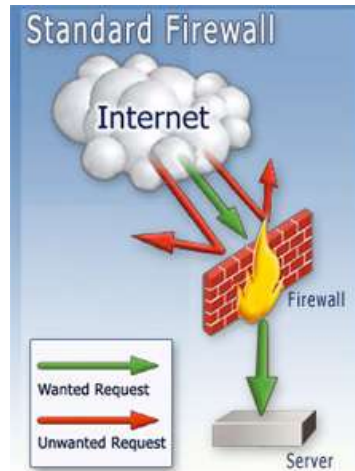


Antivirus  
Online



# Eines: Tallafocs o Firewall

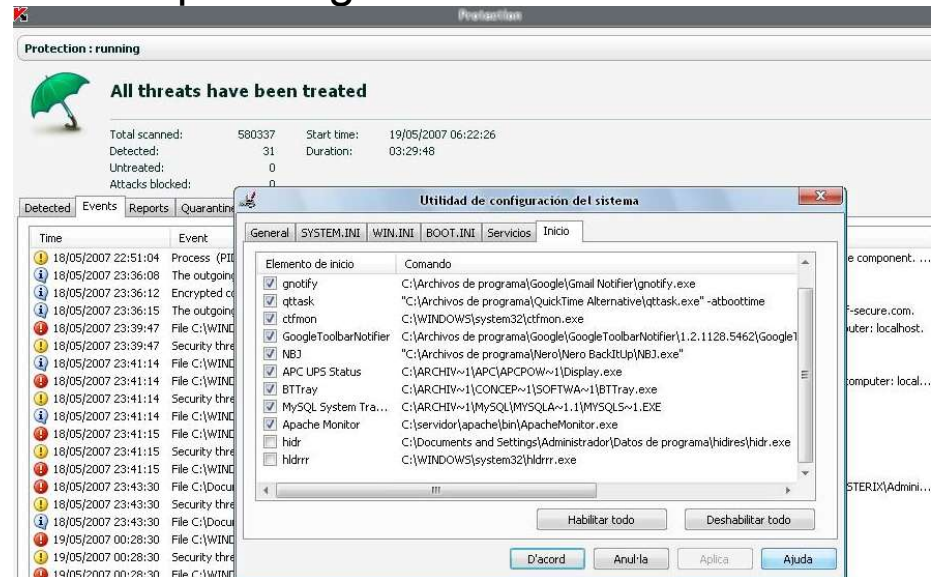
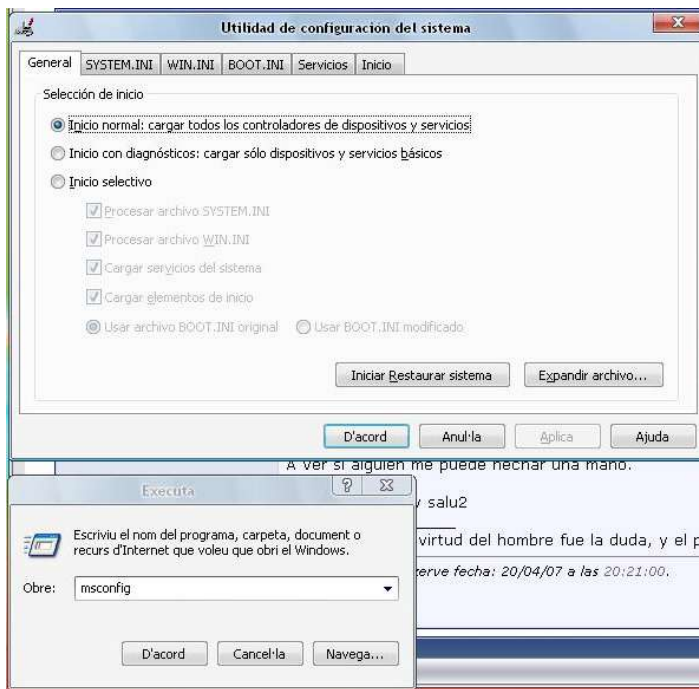
- Un tallafocs (o firewall en anglès), és un element de maquinari o programari utilitzat en una xarxa d'equips informàtics per controlar les comunicacions, permetent-les o prohibint-les segons les polítiques de xarxa, d'aquesta manera es protegeix la xarxa interna d'intents d'accés no autoritzats des d'Internet. Les comunicacions es basen en ports.





# Eines: msconfig - Deshabilitació de processos

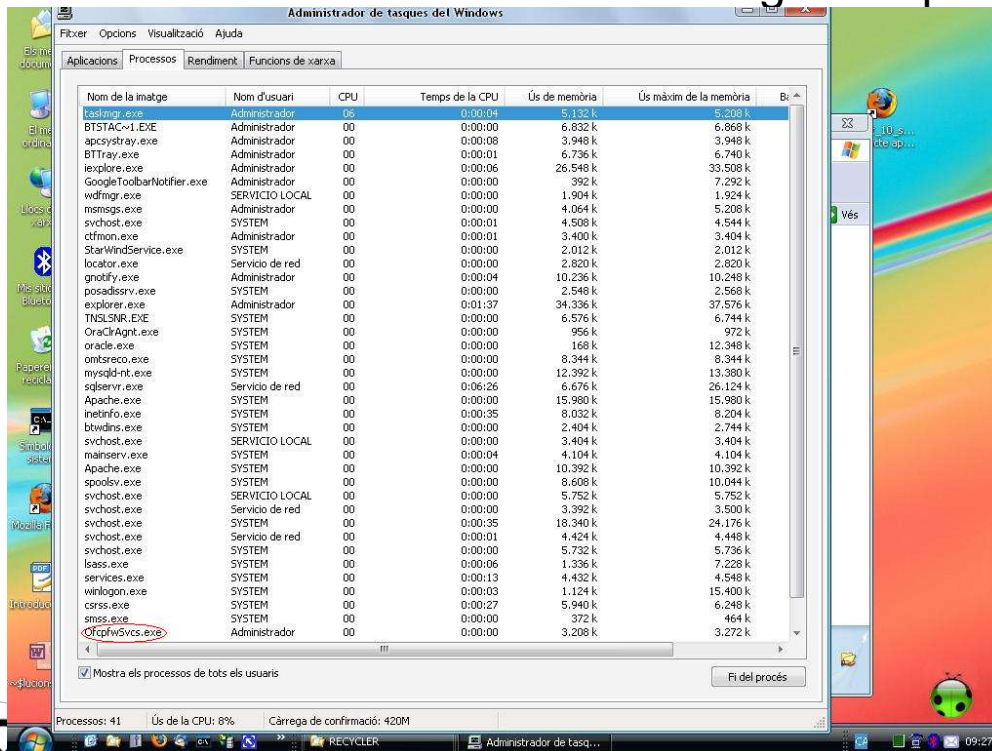
- msconfig:
  - A Inicia/Executa entrar msconfig
  - Deshabilitar processos sospitosos en la següent arrancada per tal de poder procedir a l'eliminació del virus sense que estigui en memòria.



Trojan-Downloader.Win32.Bagle: Aquest troià arriba com a adjunt a un e-mail d'spam. Quan s'executa aquest troià es fa una còpia de si mateix com HLD RRRR.EXE a la carpeta de sistema de Windows. També crea la subcarpeta %System%/EXEFLD, on guarda els arxius que descarrega d'uns quants llocs web. Aquesta rutina compromet la màquina afectada a uns altres atacs més variats i greus.

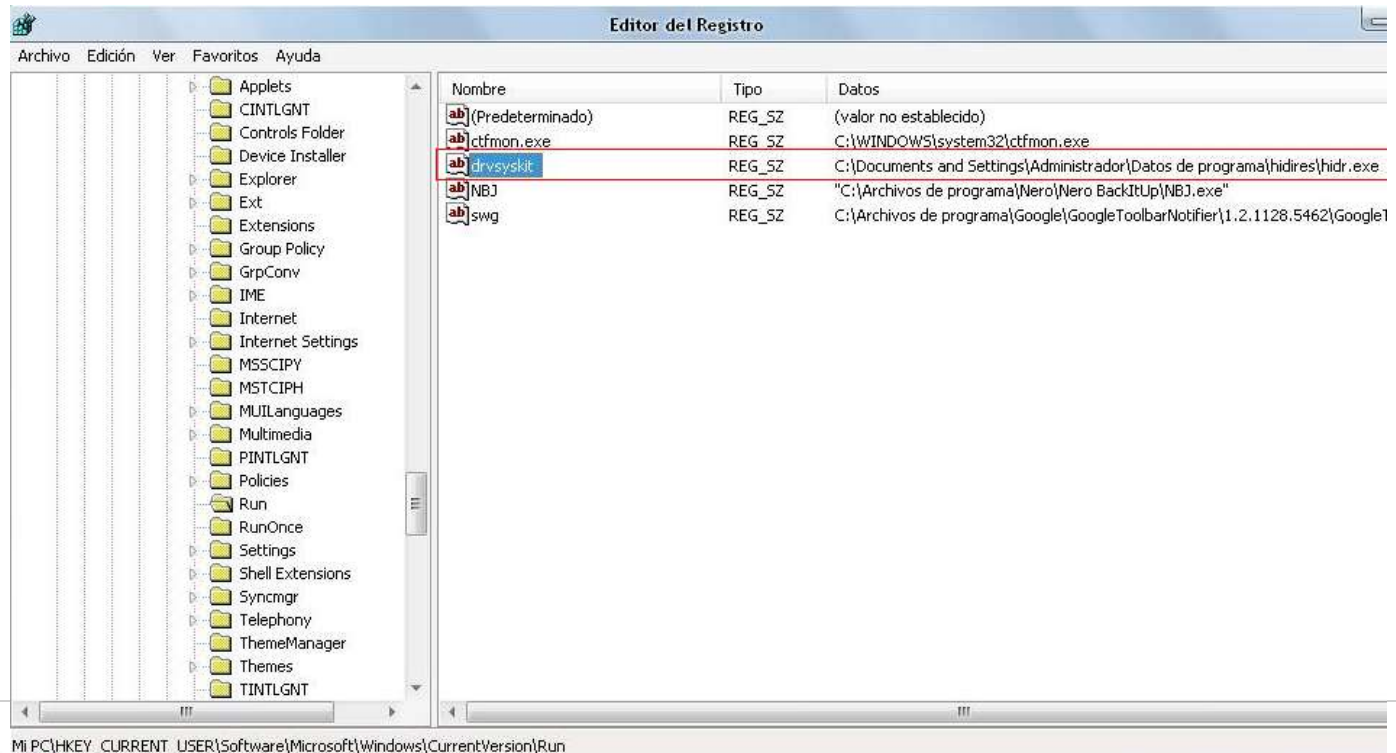
# Eines: taskmgr - Administrador de tasques

- Amb l'administrador de tasques podem veure processos sospitosos o aturar momentàniament processos de virus per tal de començar el procés d'eliminació un cop estan fora de memòria.
- Administrador de tasques:
  - A Inicia/Executa entrar taskmgr o bé prement Ctrl+Alt+Supr



# Eines: regedit - Edició manual registre

- Registre:
  - A Inicia/Executa entrar regedit
  - Buscar la clau:
    - Mi PC\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - Eliminar els virus que estiguin aquí si ja estan deshabilitats de la memòria.



# Programes espia

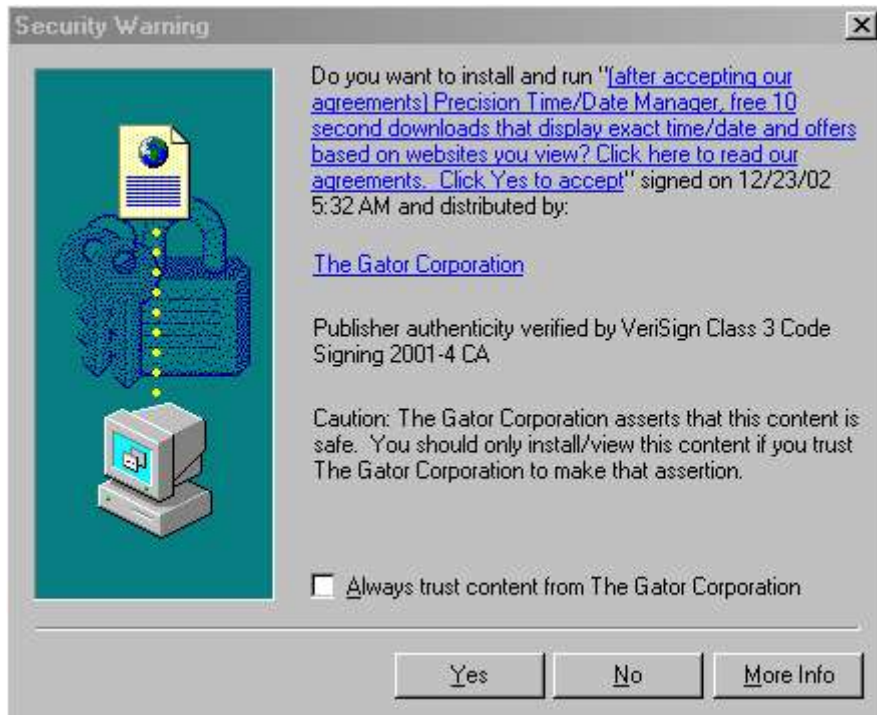
- Els **programes espia** o **spyware** són aplicacions que recopilen informació sobre una persona o organització sense el seu consentiment.
- Un cop han recopilat la informació, acostumen a distribuir-la a empreses publicitàries.
- També s'han utilitzat legalment per recopilar informació contra sospitosos de delictes, com ara en la pirateria de programari.
- Consumeix ample de banda, amb la qual cosa es pot veure afectada la velocitat de transferència de dades.
- Poden tenir accés per exemple a:
  - correu electronic
  - contrassenya
  - adreça IP
  - Telèfon
  - Pàgines visitades, amb quina freqüència es visiten
  - Programari instal·lat a l'ordinador
  - Compres fetes per Internet i amb quina tarja de crèdit
  - Comptes del bancs
  - Etc.

# Programes espia

- Es poden instal·lar:
  - Amb un virus
  - Amb un troià que es distribueixi per correu electrònic
  - Estar ocult dins la instal·lació d'un programa aparentment inofensiu.
  - Fent veure que és un programa útil mitjançant un popup o publicitat.
- Les **cookies** són fitxers en els que es guarda informació sobre un usuari que ha accedit a una web dins el propi ordinador
  - Es solen utilitzar per assignar als visitants d'una web un número d'identificació individual per reconèixer-lo més endavant.
  - Com que normalment l'usuari no sap quina informació guarda la cookie, es pot considerar una forma de spyware.
  - Aquestes dades poden ser utilitzades per seleccionar els anuncis publicitaris que es mostraran a l'usuari, o es poden trasmetre (legal o il·legalment) a altres webs.
- Exemples de programes espia: **Gator, Bonzi Buddy, Kazaa, 180 Solutions, DirectRevenue, Cydoor, CoolWebSearch, Xupiter, XXXDial and Euniverse ...**



# Programes espia



# Programes espia

- Síntomes d'infecció:
  - Canvi de la pàgina d'inici
  - Aparició de finestres "pop-ups", fins i tot sense estar connectats i sense tenir el navegador obert, la majoria de temes pornogràfics i comercials
  - Barres de cerca de webs com ara la de Alexa, Hotbar, MyWebSearch, FunWeb, etc.. que no es poden eliminar de forma fàcil.
  - Creació de carpetes tant en el directori arrel com en "Archivos de programas", "Documents and settings" i "Windows".
  - Modificació de valors del registre (especialment de la clau
  - Navegació per la xarxa cada dia més lenta
  - Tarda bastant en iniciar-se l'ordinador per culpa de la càrrega que suposo tenir molt software spyware que s'inicia quan s'engega l'ordinador (amb CCleaner es pot eliminar alteracions en el registre del sistema operatiu fetes per spyware i detecta els possibles canvis i n'informa a l'usuari).
  - Botons que apareixen a la barra d'eines del navegador i no es poden treure.
  - Aparició d'un missatge d'infecció no propi del sistema
  - Aparició d'un enllaç web per descarregar un "suposat" antispyware.
  - Quan s'accedeix a varies webs, s'oculta o es bloqueja tant el panell de control com les icones de programes.
  - Denegació de serveis de correu i missatgeria instantània



# Programes espia

- Programes antiespia
  - Actualment molts antivirus ja incorporen la capacitat d'eliminar programass espia.
  - També hi ha programes especialitzats en eliminació o bloqueig de programes espia.
  - Es recomana no utilitzar només un únic programa antiespia sinó varis, ja que sovint un detecta uns quants espies que d'altres no detecten, i viceversa.
  - Antiespies gratuïts (per ús personal):
    - Spybot - Search & Destroy
    - Ad-Aware
    - SpywareBlaster



# Altres atacs

- Phishing

- Intentar obtenir informació confidencial de forma fraudulenta (contrassenya o informació sobre targetes de crèdit o altra informació bancària).
- L'estafador (*phisher*) es fa passar una persona o empresa de confiança en una “aparent” comunicació oficial electrònica (correu electrònic, fins i tot trucades telefòniques)

The collage illustrates various phishing attempts:

- Santander Email:** A fake email from Banco Santander dated January 17, 2009, claiming a security update. It contains a link to <https://empresas.gruposantander.es/WebEmpresas/index.jsp>.
- BBVA Phishing Page:** A fake BBVA login page with fields for account number and access key. It includes a link to <http://www.ladrones.com/>.
- Firefox Browser:** A screenshot of a Mozilla Firefox browser window titled 'Ejemplo Phishing - Mozilla Firefox'. The address bar shows [http://cajamadridres.net/login\\_oi.htm](http://cajamadridres.net/login_oi.htm). The page content is a phishing attempt for Caja Madrid.
- Caja Madrid Phishing Page:** A fake Caja Madrid login page with fields for ID number, access key, and PIN. It includes a link to [http://cajamadridres.net/login\\_oi.htm](http://cajamadridres.net/login_oi.htm).

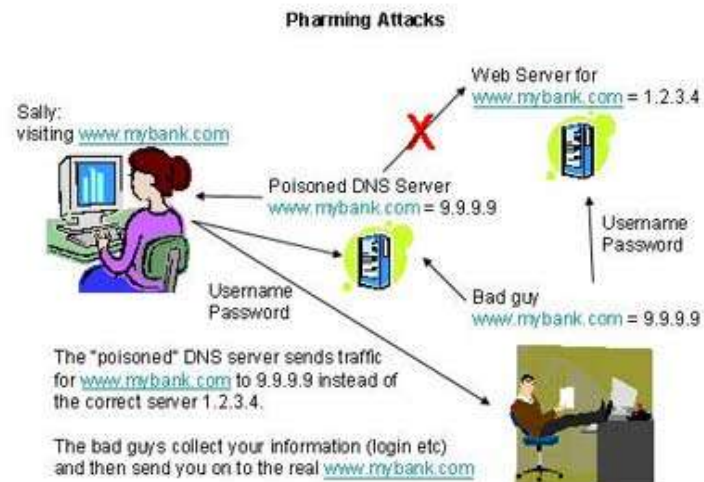
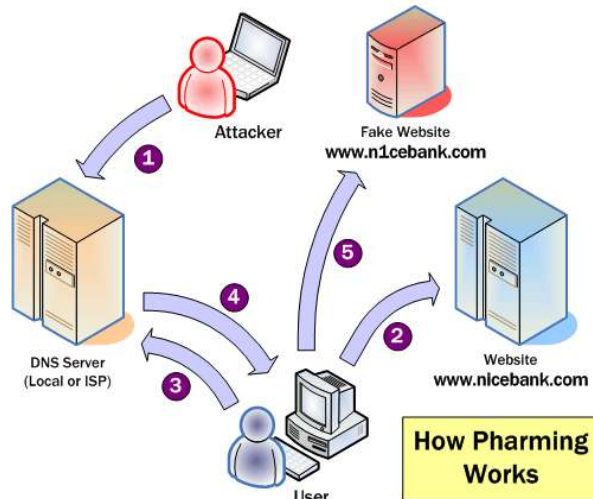
ALGUNS DRETS RESERVATS.

Joan Coll i Teixidor  
Marc Nicolau i Reixach

# Altres atacs

- Pharming

- Utilització d'una vulnerabilitat en el programari dels servidors DNS, o en el dels equips dels propis usuaris, que permet a un atacant redirigir un nom de domini a una màquina diferent.
- Així, quan un usuari introdueix un nom de domini, que ha estat redirigit, accedirà a la web que l'atacant hagi especificat per aquell nom de domini.
- Exemple:
  - Una web de banca electrònica ha estat redirigit a un altra web
  - Es mostra la mateixa aparença del a web original, demanant usuari i contrassenya per accedir als comptes del client
  - La web indica que en aquells moments no es pot accedir, però ja té capturats usuari i contrassenya!!!



# Altres atacs

- Adware
  - L'adware mostra publicitat de diferents productes i serveis no demanats expresament per l'usuari. Mostren serveis aparentment útils per l'usuari i es poden afegir com eines de recerca o pàgines inicials en navegadors per tal de que l'usuari accedeixi a les pàgines web amb més malware (tot tipus de virus i amenaces). També poden apareixer webs de casinos o de caràcter sexual.





# Altres atacs

- Obtenció de diners per coacció

**Copyright violation alert**

**Copyright violation: copyrighted content detected**

Windows has detected that you are using content that was downloaded in violation of the copyright of its respective owners. Please read the following bulletin and try solving the problem in one of the recommended ways.

**What has happened?**

During the system scan Antipiracy foundation scanner has detected copyright issues. Please take a look at the list and choose an action: pass the case to a court or settle it in pre-trial order by paying a fine.

**Files detected**

- VA-Radioplay\_Euro\_Express\_B53U-2CD-2002-SC.torrent
- Morphine + PioZone 2.torrent
- Satanic Panic 2009.DvdRip.Xvid (1337x)-Noir.torrent

**How could it happen?**

You may have been using file-sharing clients, torrents or downloaded the content in question straight from the website. In any of those cases you have violated the copyright of respective owners. In most countries this kind of action is prosecuted and serious penalties are imposed. Maximum penalties can be five years in prison and up to \$250,000 in fines.

**Lawsuits preview**

Page 1/2 Page 2/2

**Evidence list**

- HOL Network Operations Center
- Hellas On Line S.A.

**Used IPs log**

**Type of violation**

- p2p/warez movie download
- p2p/warez games download
- p2p/warez mp3 download

**Antipiracy news**

- 12/02/2010  
[New antipiracy measures are being taken against illegal content](#)
- 26/11/2009  
[Antipiracy client updated: Download version 2.0 and scan your PC for illegal and software content \(e.g. music and videos\)](#)

**Choose an action**

If you are sure that you can't have download that content to your PC or there was nothing you could do to avoid it, press "Pass the case to court" button and pass the case to court.

If these files belong to you, but you would rather avoid all the expenses associated with settling the issue in court, you can settle your case in pre-trial order by pressing "Solve..." button.

**Pass the case to court** **Settle case in pre-trial order**

[Enter a previously purchased license code](#)

<http://icpd-online.com/> - your source for copyright initiative

All rights reserved by their respective owners, 2010



Security checkout

## STATEMENT

Description	Price
Legal license purchase	\$15
Copyright holder fine	\$249
Copyright protection organization fee for the use of software tracking illegal file downloads	\$126
Traffic fee	\$2
	\$7.85
<b>Total:</b>	<b>\$399.85</b>

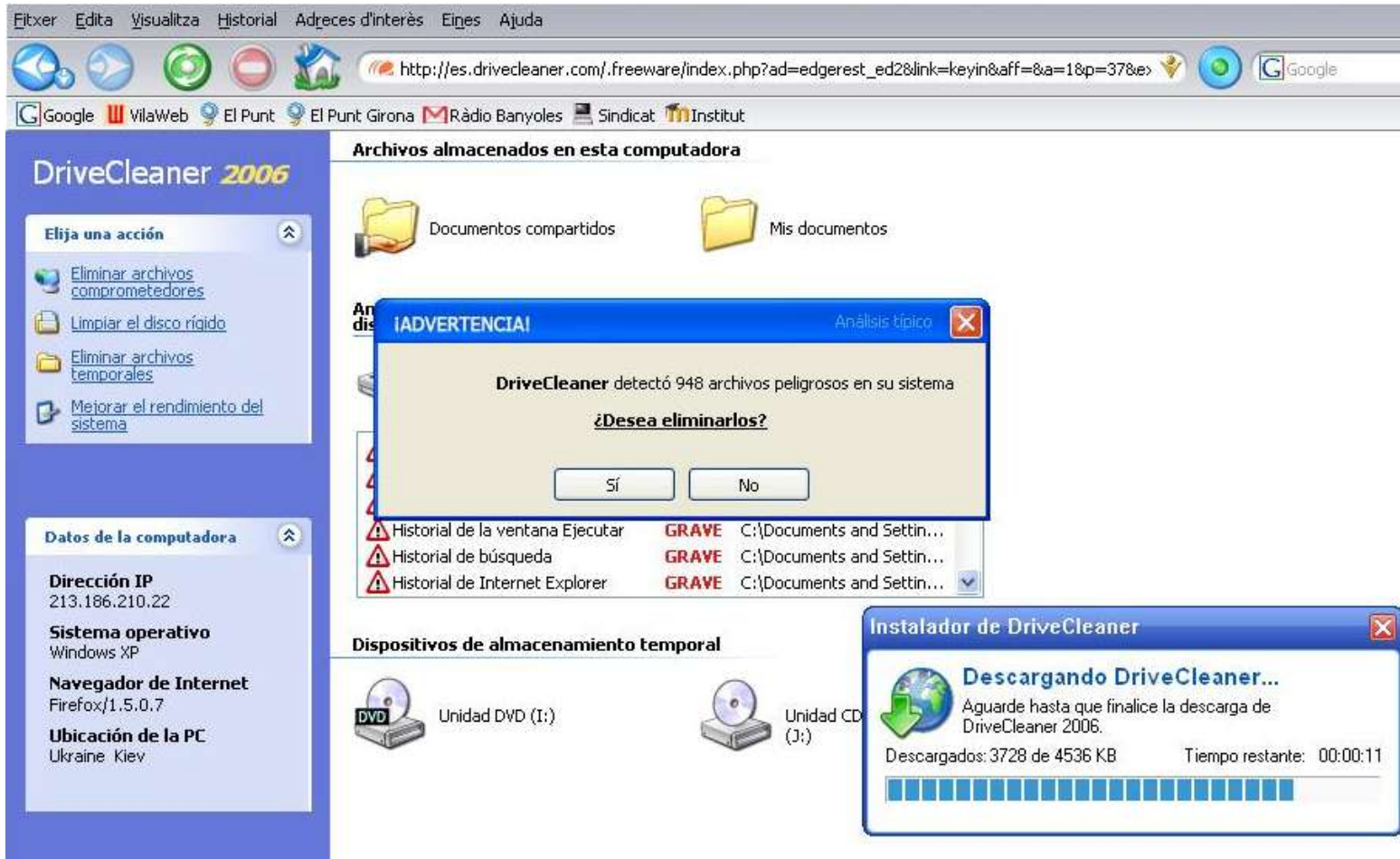
# Altres atacs

- Instal·lació forçada de programa per esgotament de l'usuari
  - Hi ha publicitats en pàgines web que obren noves pàgines amb programes on quasi no hi ha més opció que instal·lar el programa ja que qualsevol opció Si/No l'instal·la. Pot ser un malware o bé un programa comercial per comprar mitjançant la por.

The collage shows three main deceptive advertisements:

- SystemDoctor 2006:** A web page with a large yellow banner and a doctor character. A red circle highlights a button that says "¡Haga clic aquí para analizar!". Below it, a red circle highlights a section titled "Errores de sistema detectados: 257". A pop-up window shows a message: "La página a http://es.systemdoctor.com diu: IMPORTANTE: El análisis no ha finalizado. La presencia de virus en su computadora podría causar funcionamiento errático o impredecible, bloqueos del sistema y pérdida de datos. Instale SystemDoctor para detectar y eliminar los virus de su sistema. (Recomendamos la instalación inmediata)." with "D'acord" and "Cancel·la" buttons.
- DriveCleaner:** A web page with a blue banner. A red circle highlights a button that says "Eliminar archivos comprometidos". A pop-up window shows a message: "La página a http://es.systemdoctor.com diu: IMPORTANTE: El análisis no ha finalizado. La presencia de virus en su computadora podría causar funcionamiento errático o impredecible, bloqueos del sistema y pérdida de datos. Instale SystemDoctor para detectar y eliminar los virus de su sistema. (Recomendamos la instalación inmediata)." with "D'acord" and "Cancel·la" buttons.
- Drive Cleaner:** A web page with a blue banner. A red circle highlights a button that says "Haga clic aquí para liberar el poder de limpieza de DriveCleaner". A pop-up window shows a message: "¡ADVERTENCIA! Se encontraron 18454 amenazas a su privacidad. DriveCleaner encontró 18454 amenazas en su computadora la última vez que realizó una limpieza de sistema. ¡Es necesario eliminarlas de inmediato!" with "Fals" and "Comprar ahora" buttons.

# Altres atacs



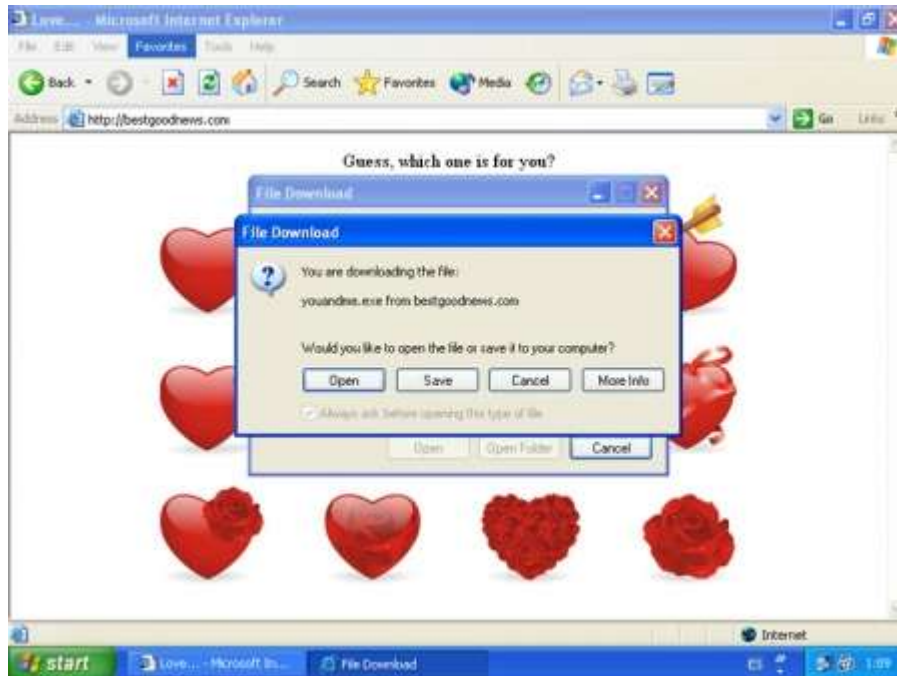


# Altres atacs

The screenshot shows a web browser window displaying the SystemDoctor 2006 website. The browser's address bar shows the URL: `http://es.systemdoctor.com/download/2006/index.php?aid=ifdidnit_rdt_ed2&lid=keyin&ex=1&p=19`. The website has a yellow header with the "systemdoctor 2006" logo. Below the header, there is a large button that says "¡Haga clic aquí para analizar!". To the right of this button is an illustration of a doctor in a white coat and stethoscope, holding a computer monitor. Below the button, a progress bar is shown, followed by the text "Errores de sistema detectados: 257". To the left of the doctor illustration, there is a list of checked items: "Verificación del registro", "Verificación exhaustiva del registro", "Accesos directos de aplicaciones", and "Errores del disco rígido". To the right of the doctor illustration, there is a section titled "Información importante:" which states: "Al hacer estará aceptando el Contrato de licencia del programa." Below this, there are two sections: "SystemDoctor 2006 detecta y elimina errores en:" and "Repara archivos dañados: de Excel, de imagen, video y otros recuperar información y archivos multimedia que creía perdidos". Overlaid on the right side of the browser window is a Firefox "Traffic Monitor: training" window. This window shows an "Outgoing encrypted connection" to "Firefox" with a "Remote address" of "140.211.166.205" and a "Remote port" of "443". It also shows a "Scan encrypted connection" section with a checkbox for "Apply to all" and buttons for "Process" and "Skip". A message from Kaspersky Internet Security is visible: "Kaspersky Internet Security can scan this encrypted connection for viruses. Do you want this connection to be scanned?"

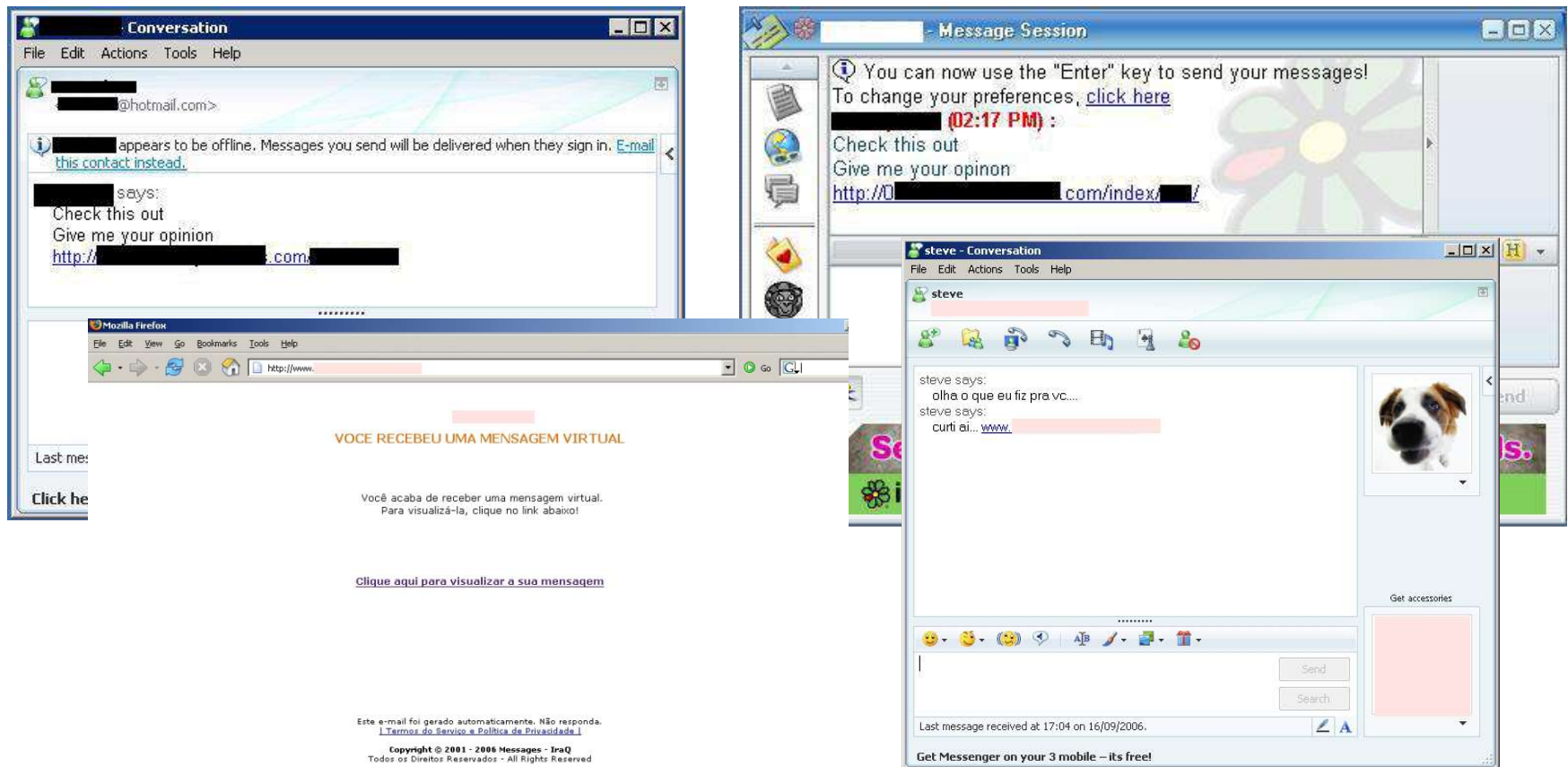
# Altres atacs

- Enllaços trampa



# Altres atacs

- Missatgeria instantània (IM virus o bot IM)
  - Utilitzen programes de missatgeria instantània (messenger, skype,...) per enviar enllaços a pàgines web on hi ha algun tipus de virus (ex. Culler, MSN Diablo, Hakaglan)



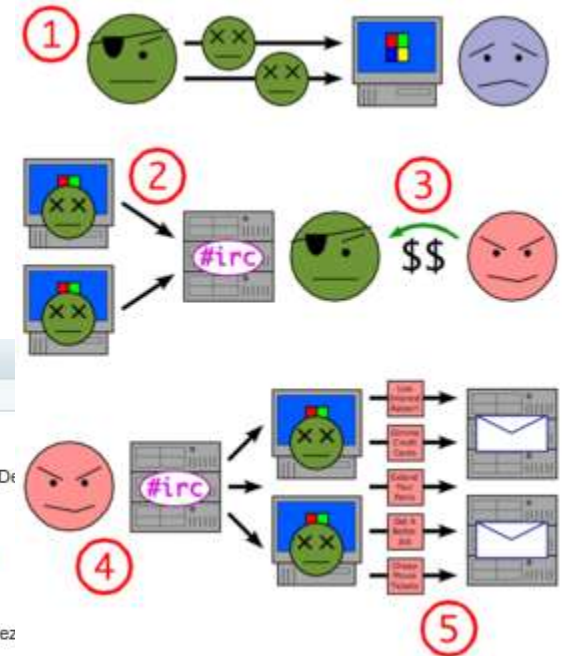


# Altres atacs

- Bots i Botnet (robots i robots en xarxa)
  - Són programes que s'executen de manera autòmata i poden esperar ordres perquè l'atacant des de l'exterior pugui controlar un ordinador o un conjunt important d'ordinadors alhora per fer un atac, enviar correu escombraria, virus o missatgeria instantània



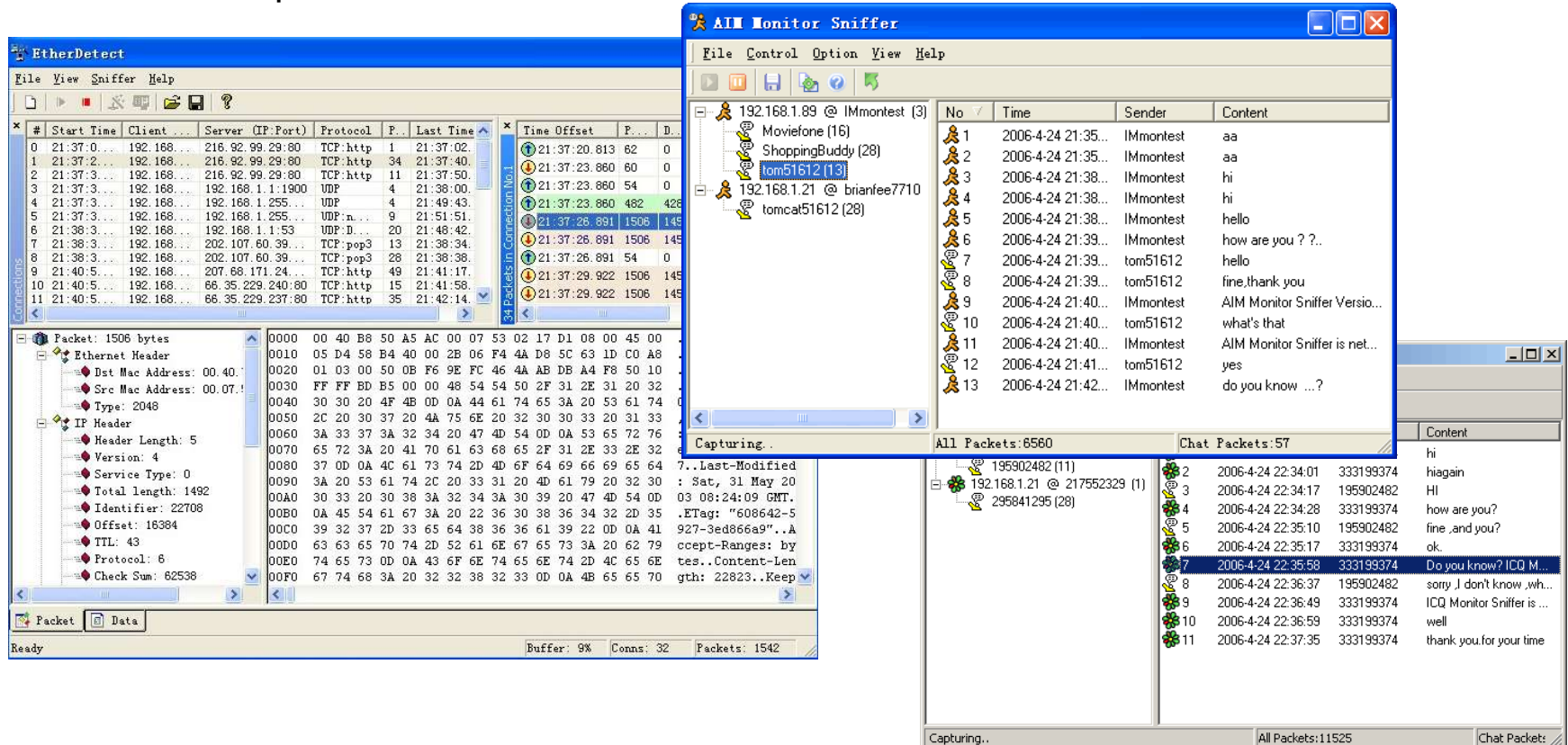
The screenshot shows a Gmail interface with a spam message from 'Pilar' containing a link to 'http://www.espana2.net'. Below the email, there is a forum post from 'Ruby Forum' with the same link. To the right, there is a 'Weblinks' section with various links, including 'www.amigoscordoba.info' and 'Fundación Centro Tecnológico da Carne'.



# Altres atacs

- Sniffers

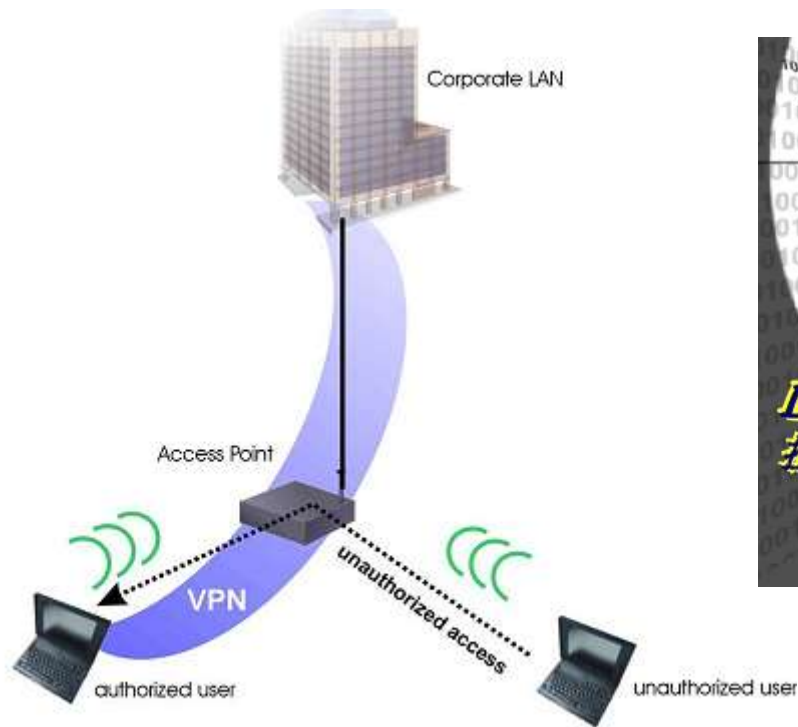
- Són programes que capturen i permeten analitzar tot el trànsit que circula per la xarxa. Poden capturar informació sensible com ara contrasenyes i missatges de text no encriptats.





# Altres atacs

- Atacs WIFI
  - Hi ha programes que permeten entrar a xarxes mitjançant l'accés inalàmbtric o WIFI.



# Altres atacs

- Atacs DoS (Denial of Service)
  - Un atac de denegació de servei o DoS és un atac a un sistema d'ordinadors o xarxa que fa que un servei o recurs sigui inaccessible. El poden fer un o varis ordinadors alhora. També es sol utilitzar per fer caure servidors d'Internet.

