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, hoaxs, 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**

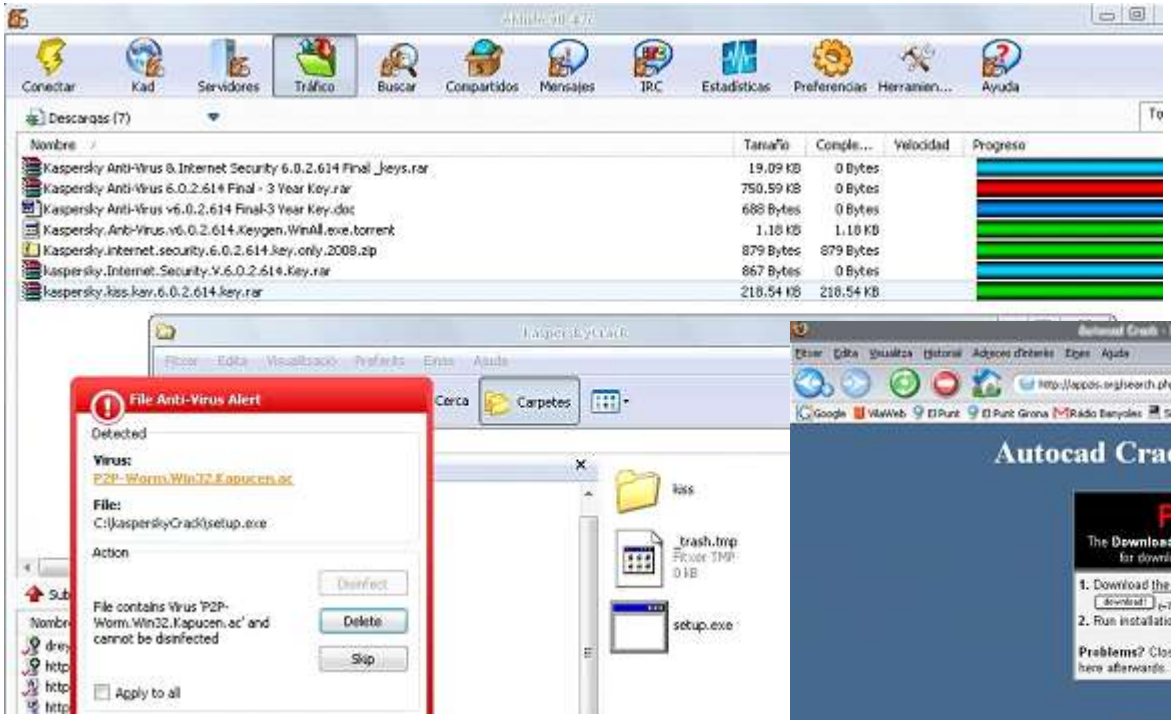
Virus

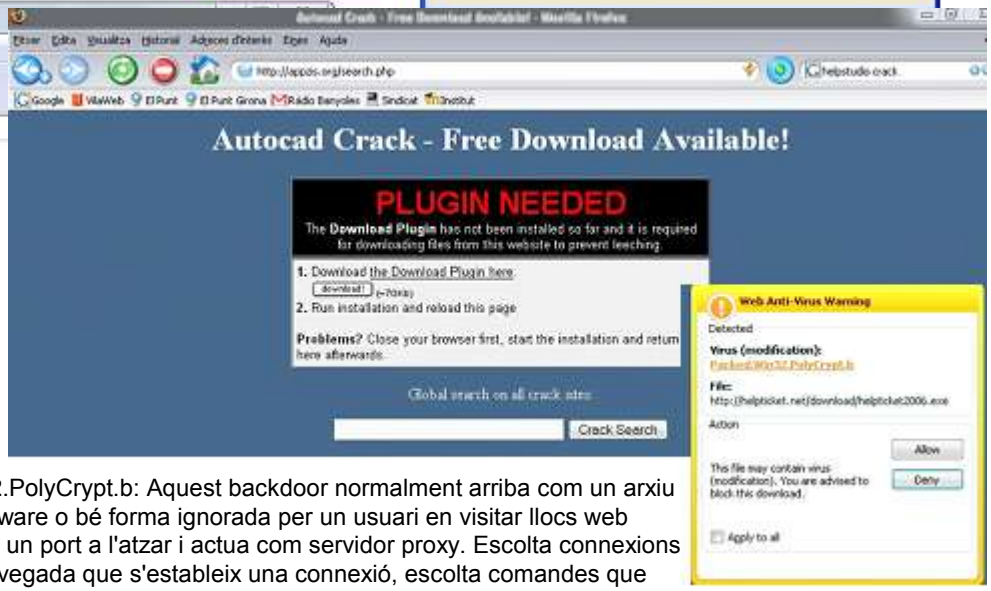
- Un **virus informàtic** és un programa que té per objectiu alterar el funcionament normal de l'ordinador, sense permís o coneixement de l'usuari.
- Són programes que es poden replicar i executar per sí mateixos.
- Normalment, substitueixen fitxers executables per altres d'infectats amb el codi del 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 ilícites 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

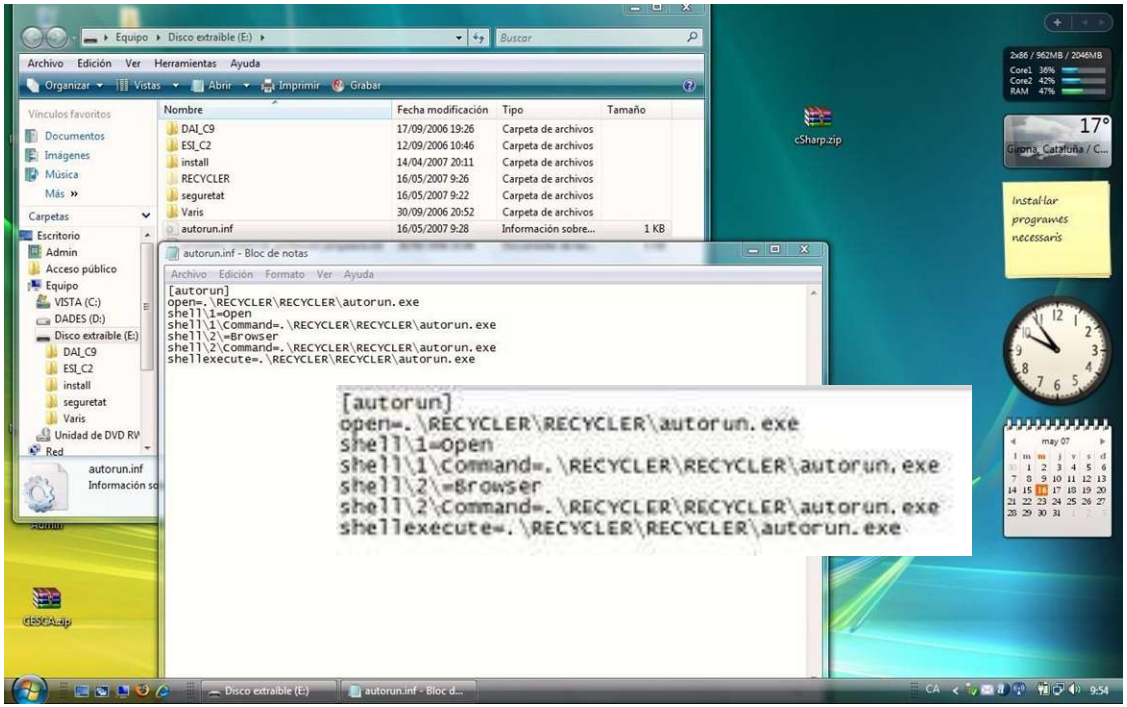




WORM_KAPUCEN: Aquest cuc normalment arriba en un sistema amb un arxiu descarregat des d'aplicacions peer-to-peer (P2P). Busca unes quantes carpetes de P2P, i es copia a si mateix utilitzant un nom d'arxiu específic, RAR o arxiu .ZIP per poder-se propagar fàcilment. També crea un arxiu de .TXT, que conté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

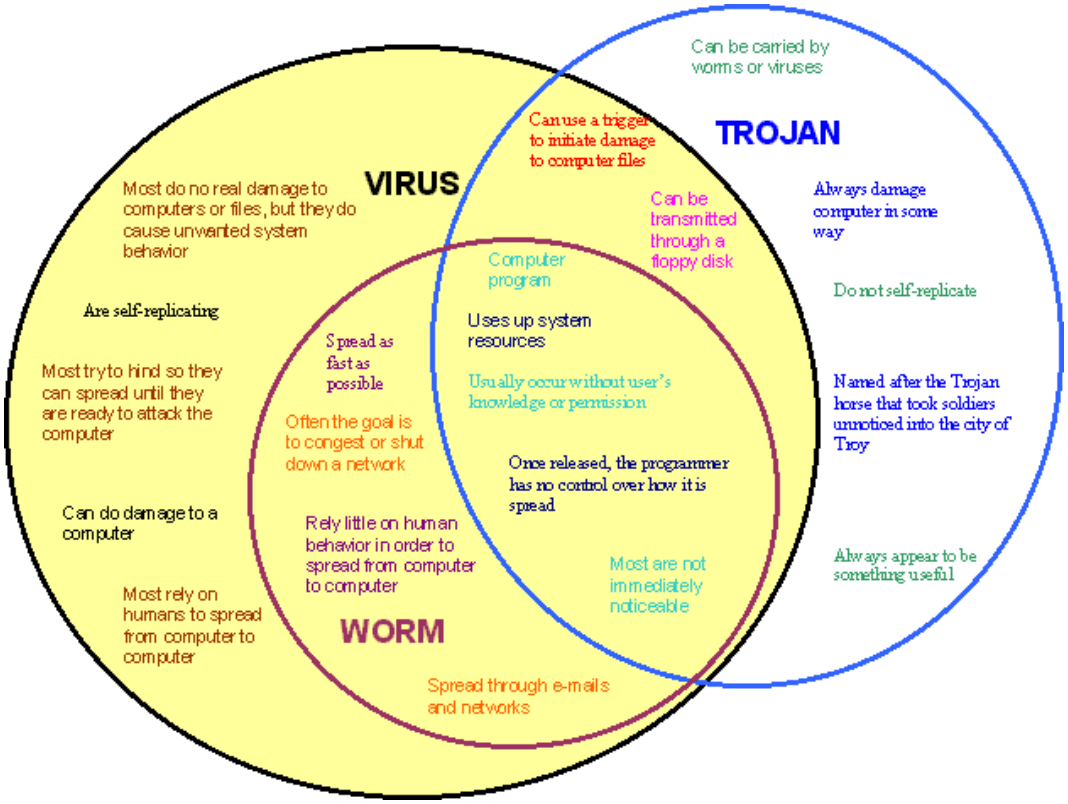
L'atacant pot entre d'altres coses

* 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**
  - 1ª 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)*.
  - 2ª 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.
  - 3ª 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 (Troià) , 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'extèn per enviament de correu massiu,

Classificació dels virus

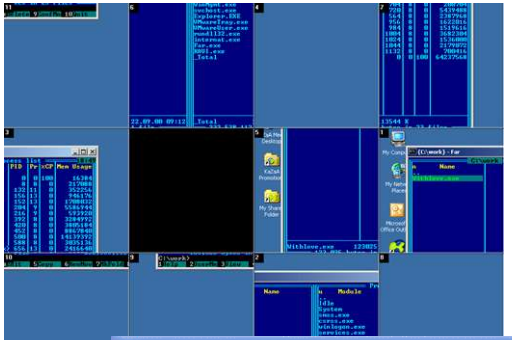


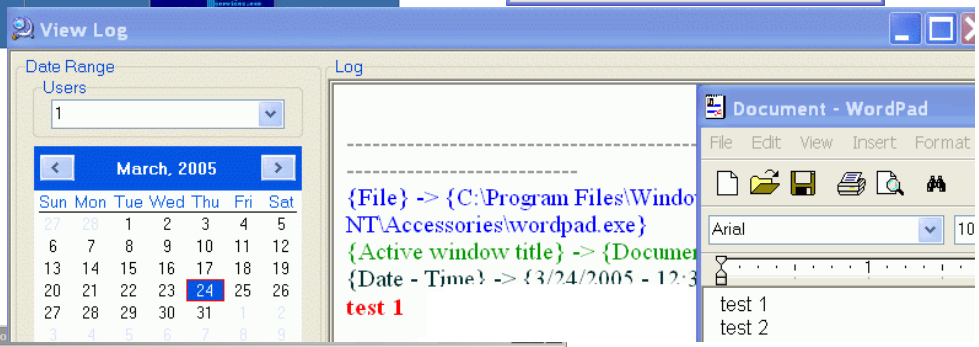
Classificació dels virus

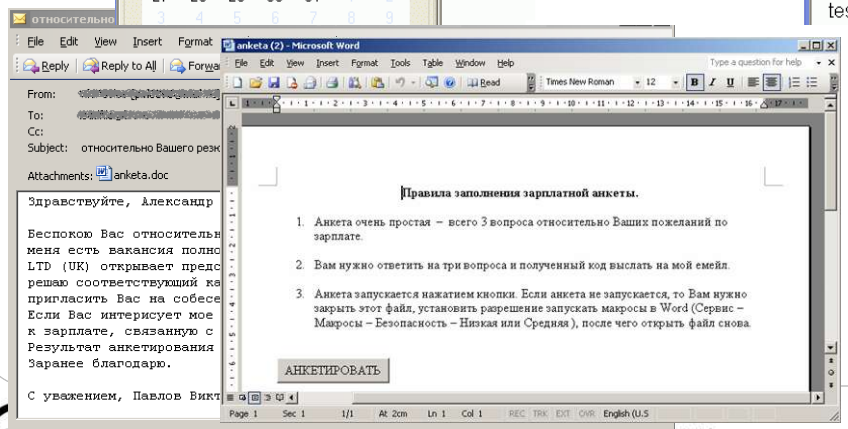
- **Tipus de virus**
  - *Worms* o cucs
    - S'executen quan inicia el sistema operatiu, ocupant memòria i alentint l'ordinador
    - No infecten altres fitxers executables.
    - Utilitzen medis massius com el correu electrònic per propagar-se.
  - Troians
    - Solen ser els més perillosos.
    - 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 fitrxers 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

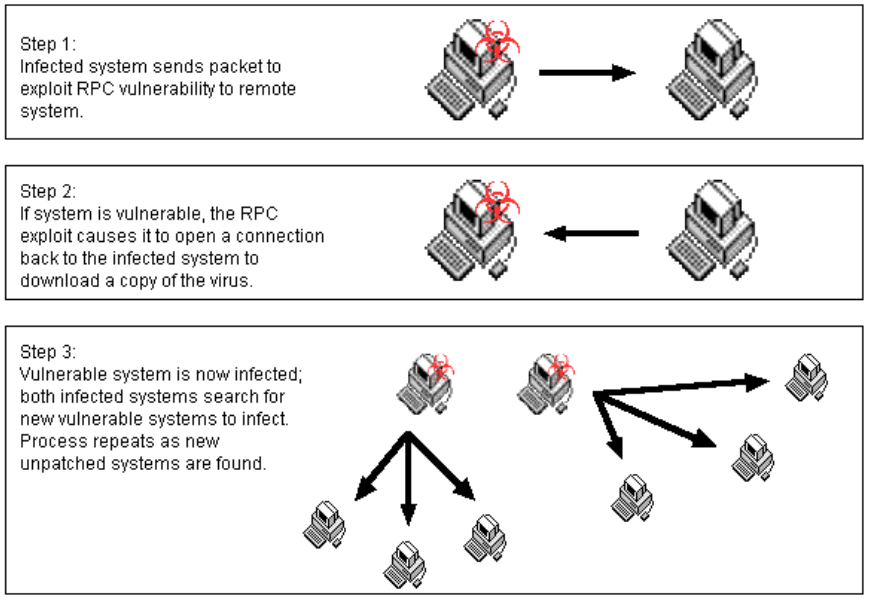


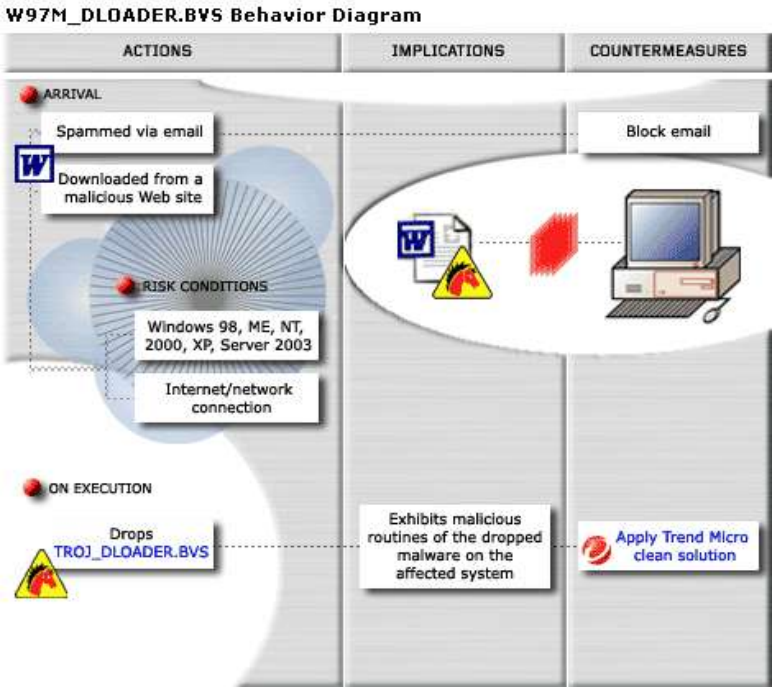




Joan Coll i Teixidor
Marc Nicolau i Reixach

Propagació de virus





Símptomes 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 "estranys"
- Disminució de la RAM accessible per treballar.
- Sons o vídeos amb efectes estranys

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
    - En aquesta web en castellà es pot cercar un virus i ens dóna informació sobre el "mal" que provoca i la seva solució.

Com treure un virus de l'ordinador?

Eines: Antivirus

- Programas 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).

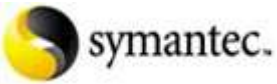
Eines: Antivirus

- 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.

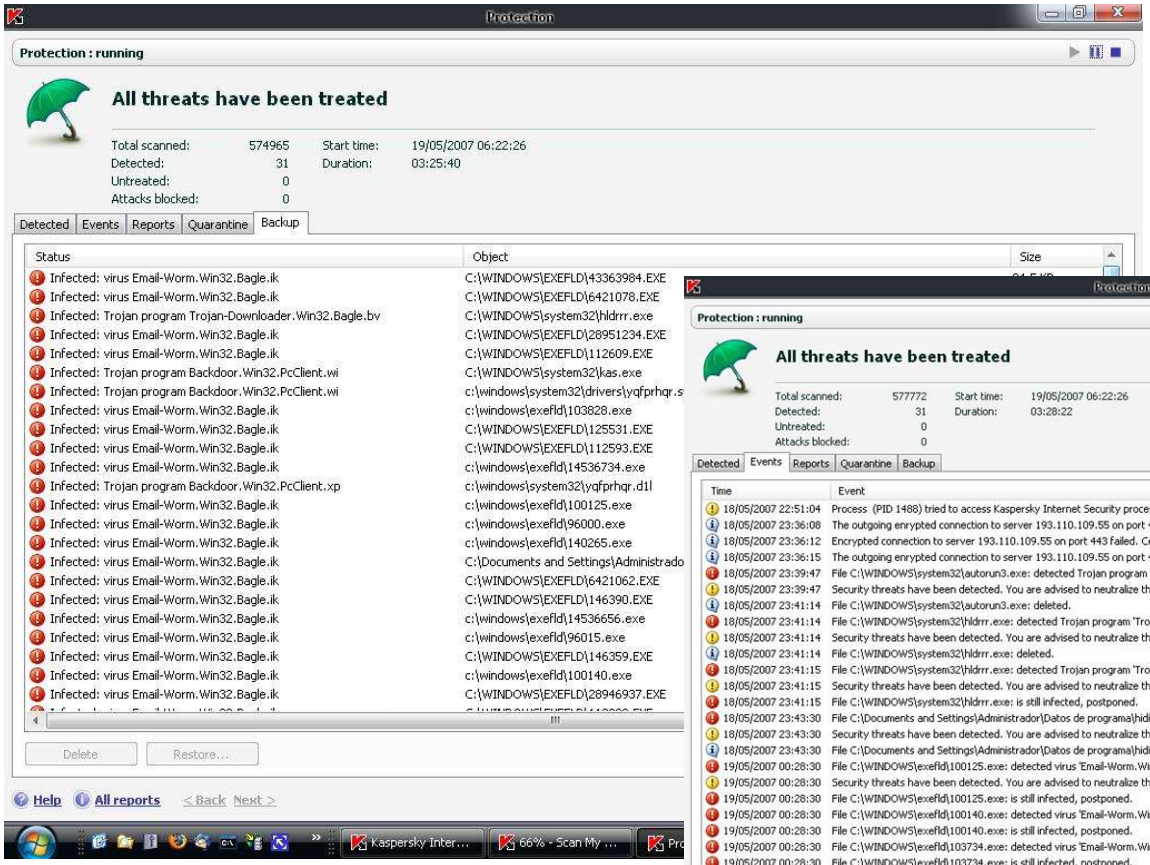
Eines: Antivirus

- 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

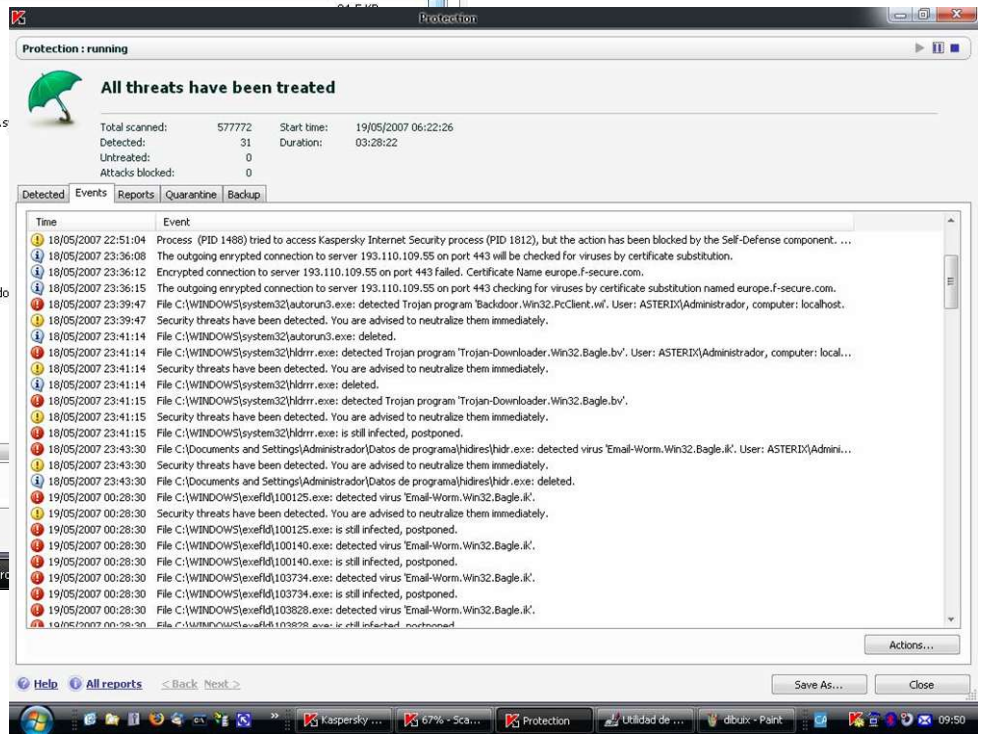
Eines: Antivirus



Eines: Antivirus

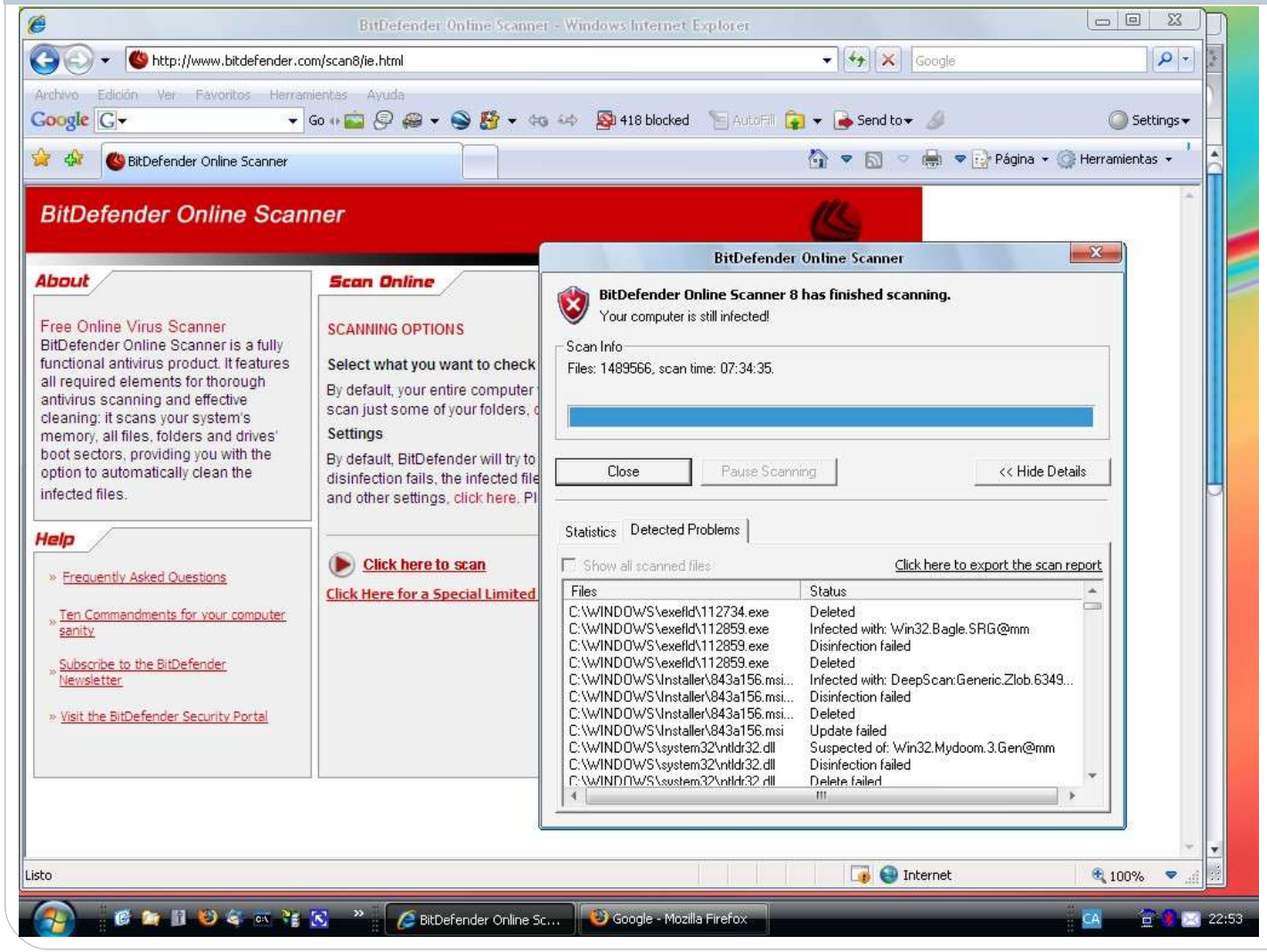


Antivirus local



Eines: Antivirus

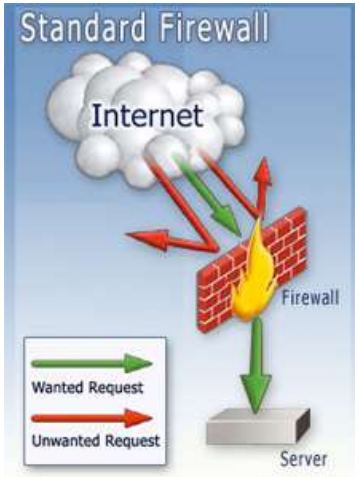
Eines: Antivirus

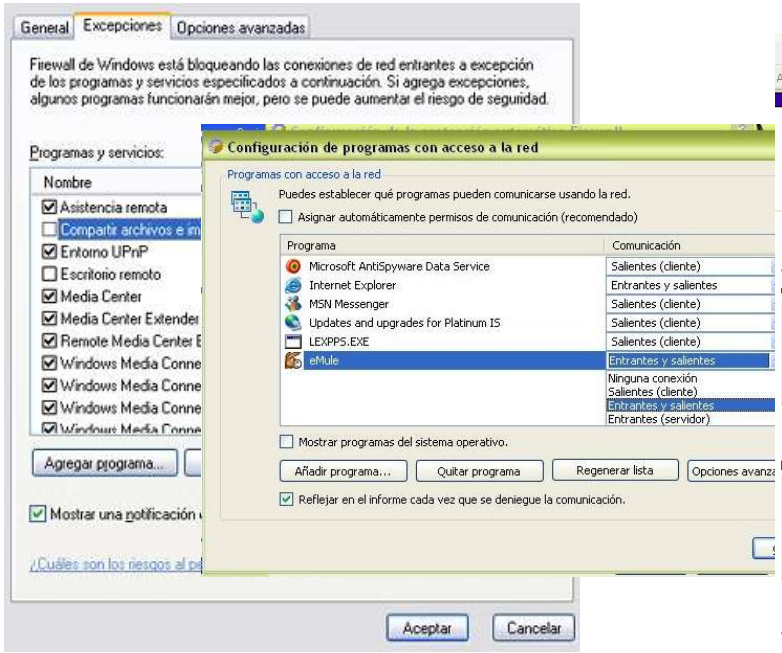


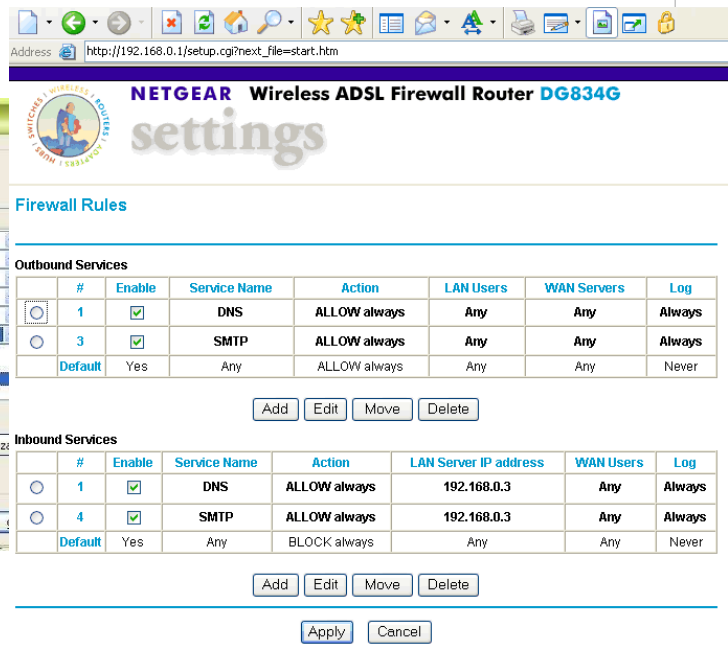
Antivirus Online

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.

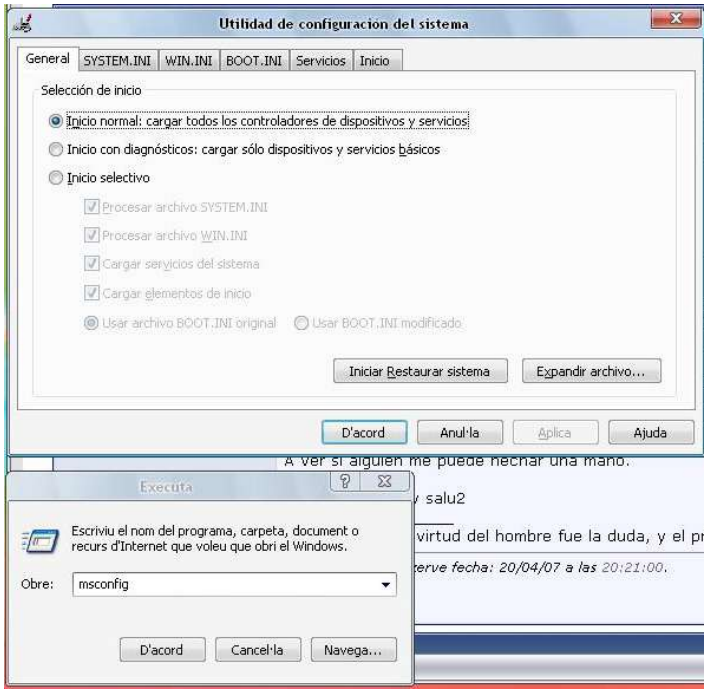


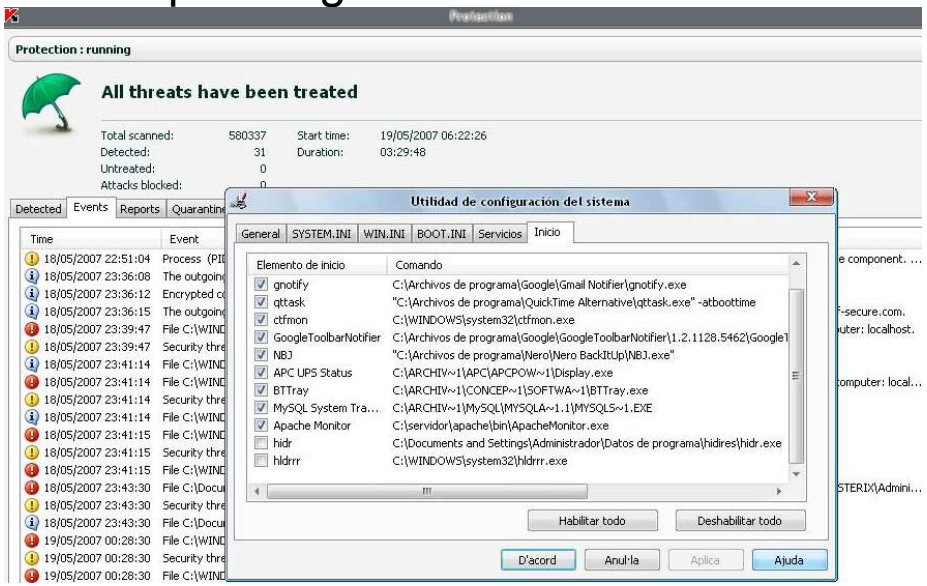




Eines: msconfig - Deshabilitació de processos

- 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.

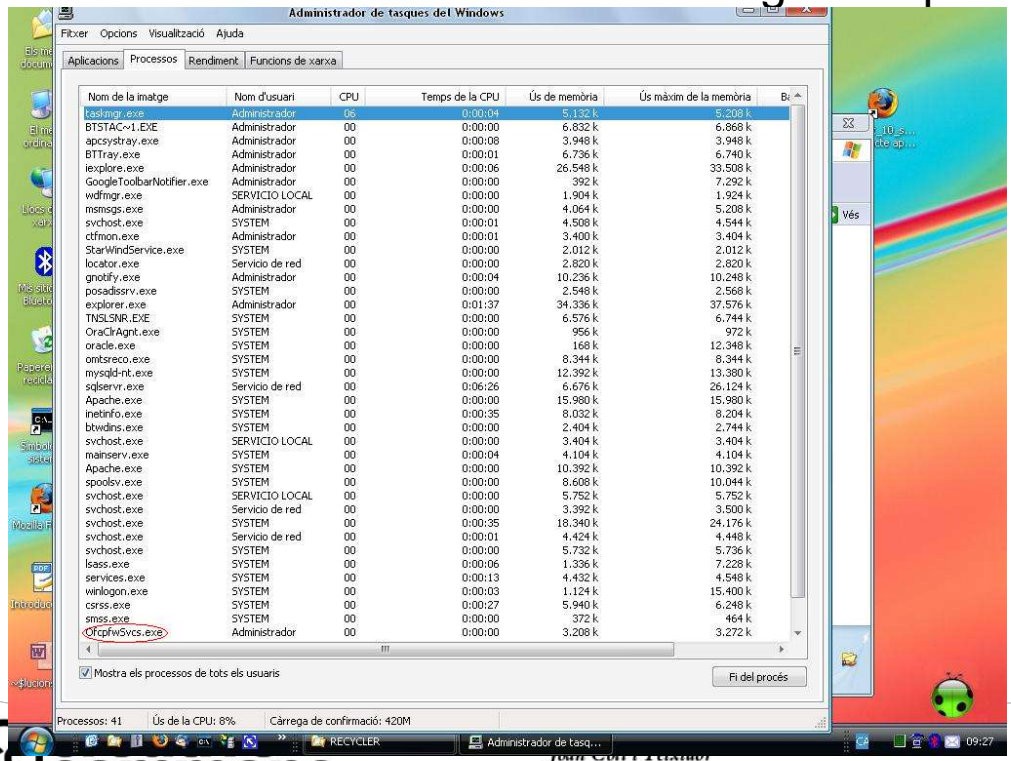




Trojan-Downloader.Win32.Bagle: Aquest troià arriba com a adjunt a un e-mail d'spam.Quan s'executa aquest troià es fa una còpia de si mateix com HLDRRR.EXE a la carpeta de sistema de Windows. També crea la subcarpeta %System%/EXEFLD, on guarda els arxius que descarrega d'uns quants llocs web. Aquesta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

Eines: taskmgr - Administrador de tasques

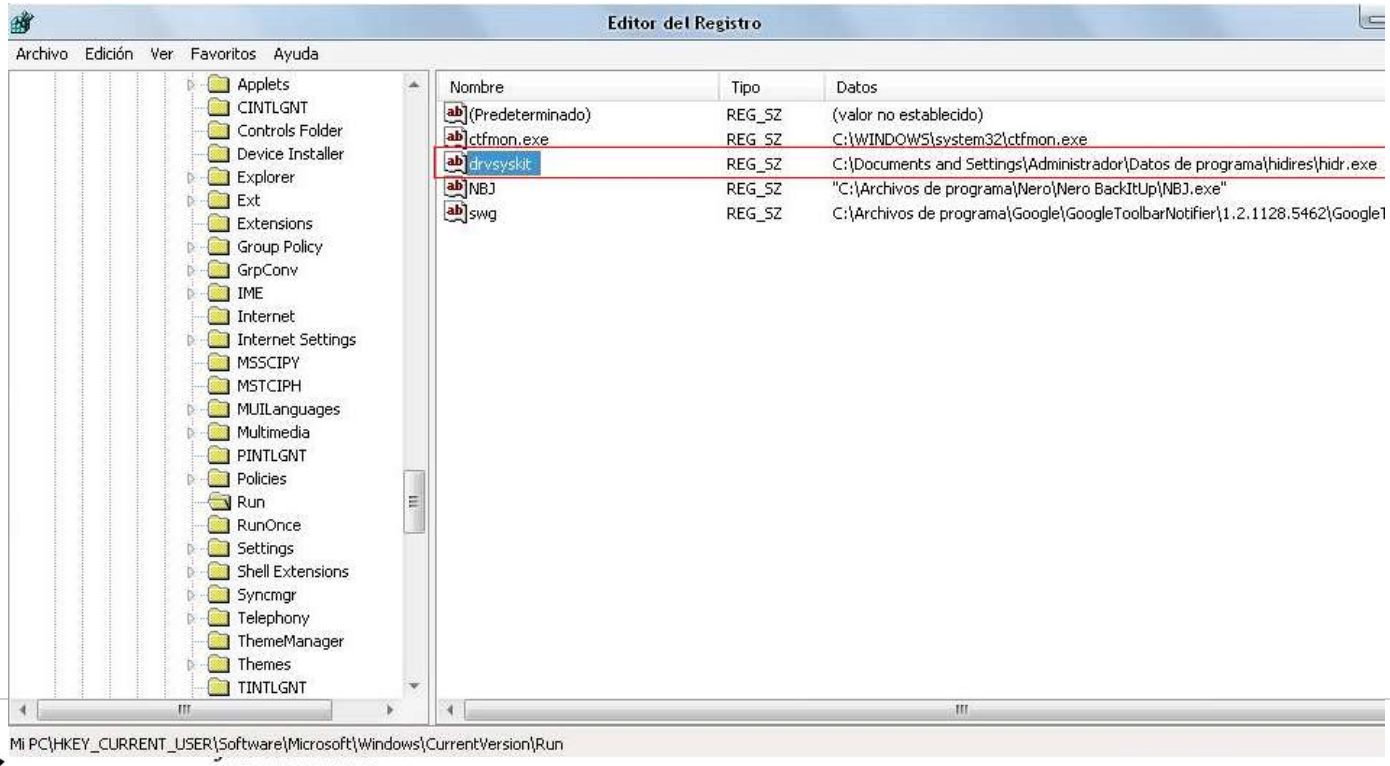
- Amb l'administrador de tasques podem veure processos sospitosos o aturar momentàniament processos de virus per tal de començar el procés d'eliminació un cop estan fora de memòria.
- Administrador de tasques:
  - A Inicia/Executa entrar taskmgr o bé prement Ctrl+Alt+Supr



Marc Nicolau i Reixach

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 aqui 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 publicitaries.
- 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 electronic
  - 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 reconeixer-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 ilegalment) a altres webs.
- Exemples de programes espia: **Gator**, **Bonzi Buddy**, **Kazaa, 180 Solutions, DirectRevenue, Cydoor, CoolWebSearch, Xupiter, XXXDial and Euniverse** ...

Programes espia

Programes espia

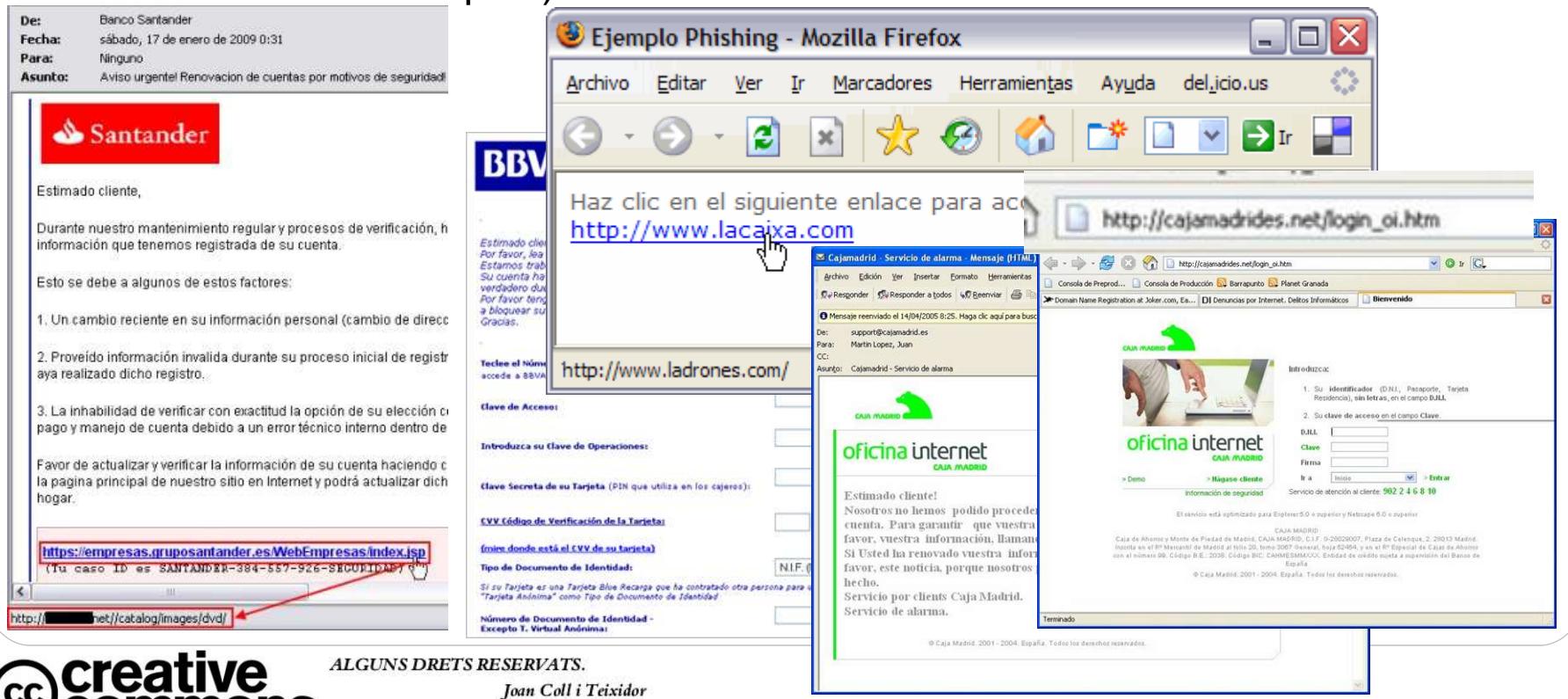
- Símptomes d'infecció:
  - Canvi de la pàgina d'inici
  - Aparició de finestres "pop-ups", fins i tot sense estar connectats i sense tenir el navegador obert, la majoria de temes pornogràfics i comercials
  - Barres de cerca de webs com ara la de Alexa, Hotbar, MyWebSearch, FunWeb, etc.. que no es poden 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 programas 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

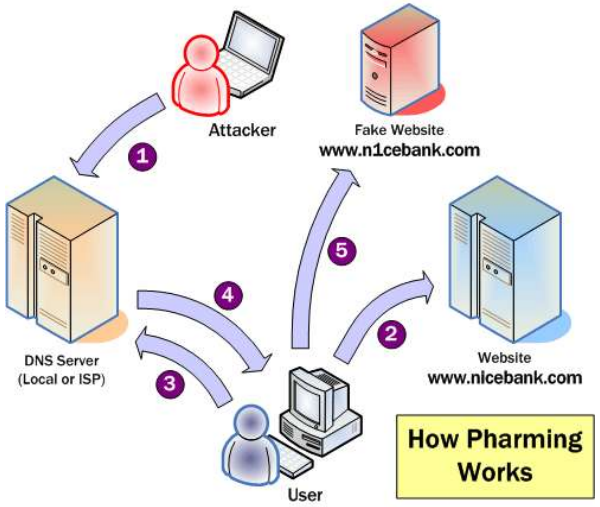
Altres atacs

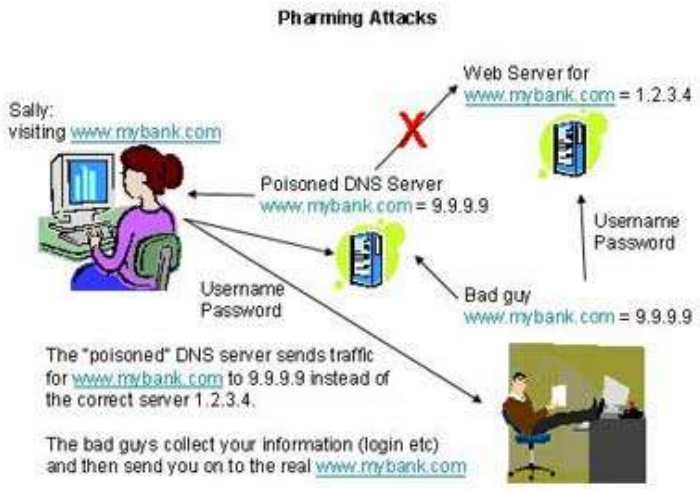
- Phishing
  - Intentar obtenir informació confidencial de forma fraudulenta (contrassenya o informació sobre targes de crèdit o altra informació bancaria).
  - L'estafador (*phisher)* es fa passar una persona o empresa de confiança en una "aparent" comunicació oficial electrònica (correu electrònic,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



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 redireccionar un nom de domini a una màquina diferent.
  - Així, quan un usuari introdueix un nom de domini, que ha estat redireccionat, accedirà a la web que l'atacant hagi especificat per aquell nom de domini.
  - Exemple:
    - Una web de banca electrònica ha estat redireccionada 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.

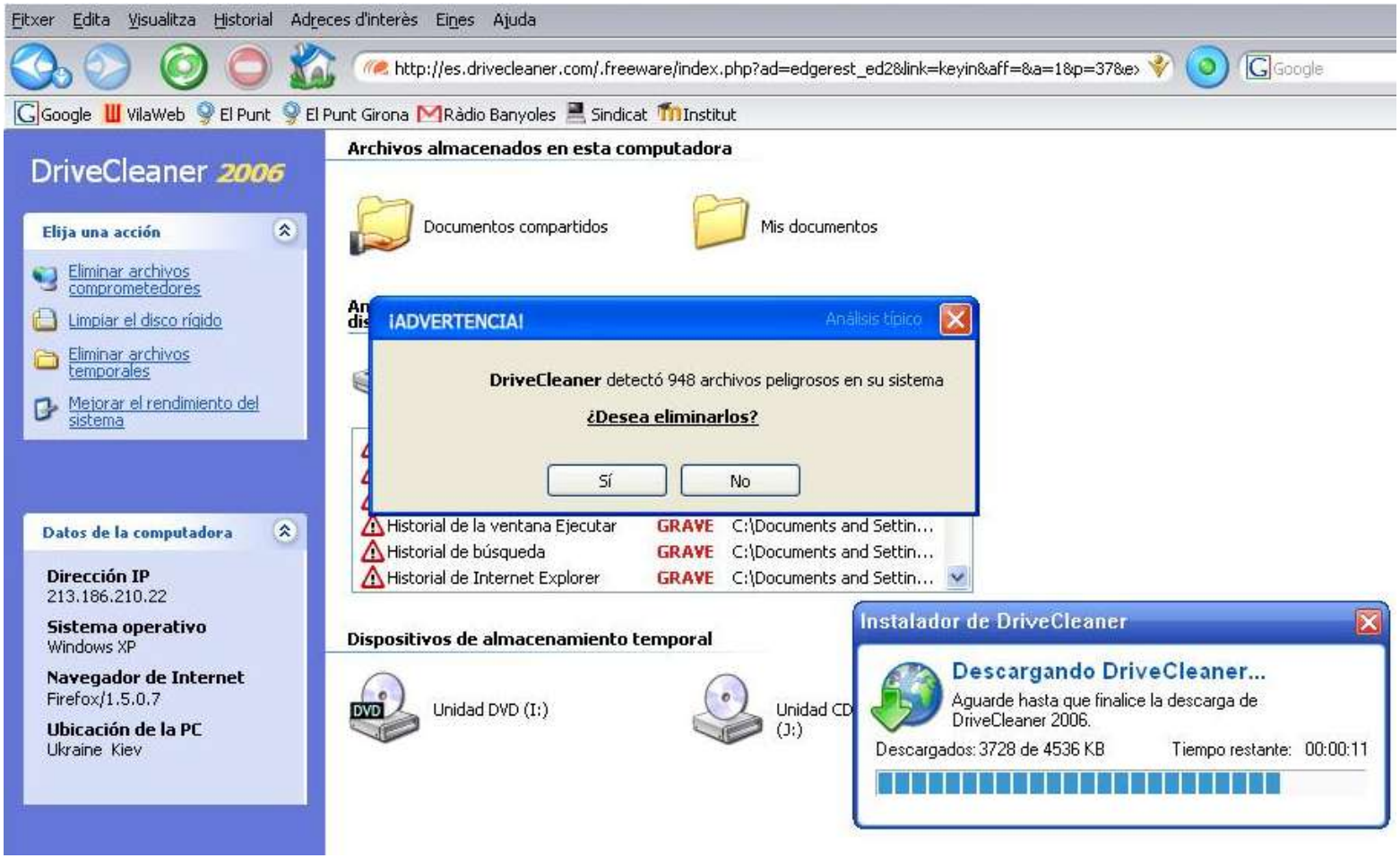
Altres atacs

- Obtenció de diners per coacció

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.

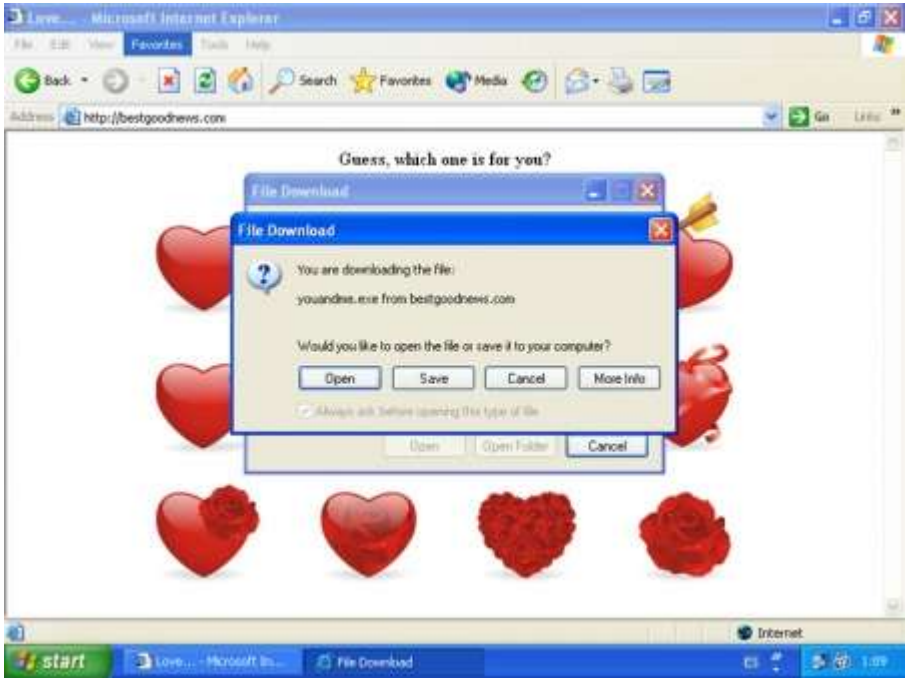
Altres atacs



Altres atacs

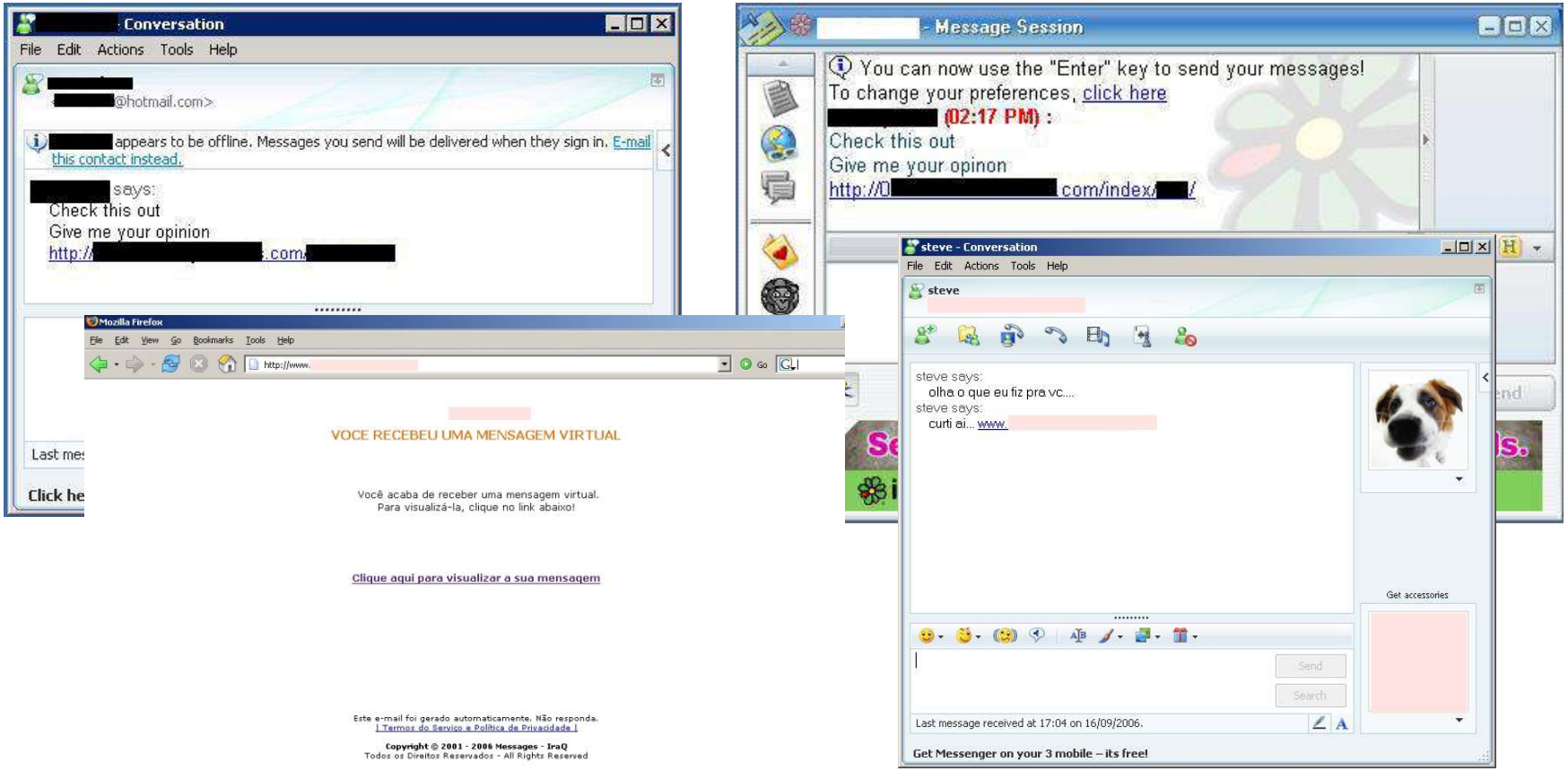
Altres atacs

- Enllaços trampa



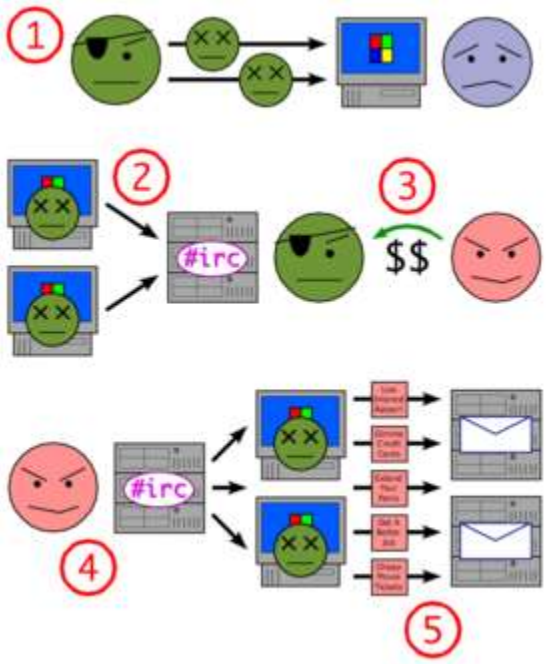
Altres atacs

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



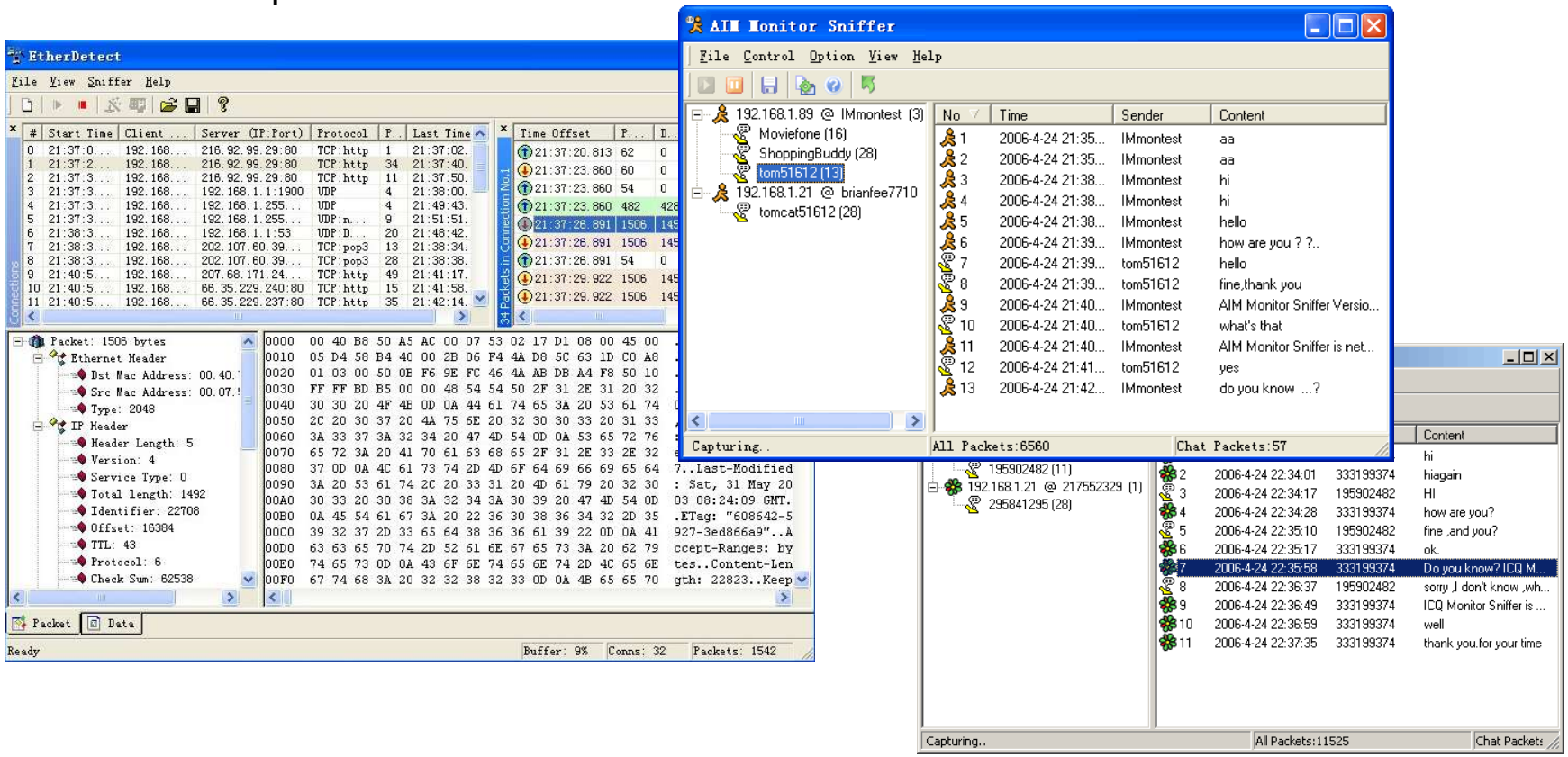
Altres atacs

- 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



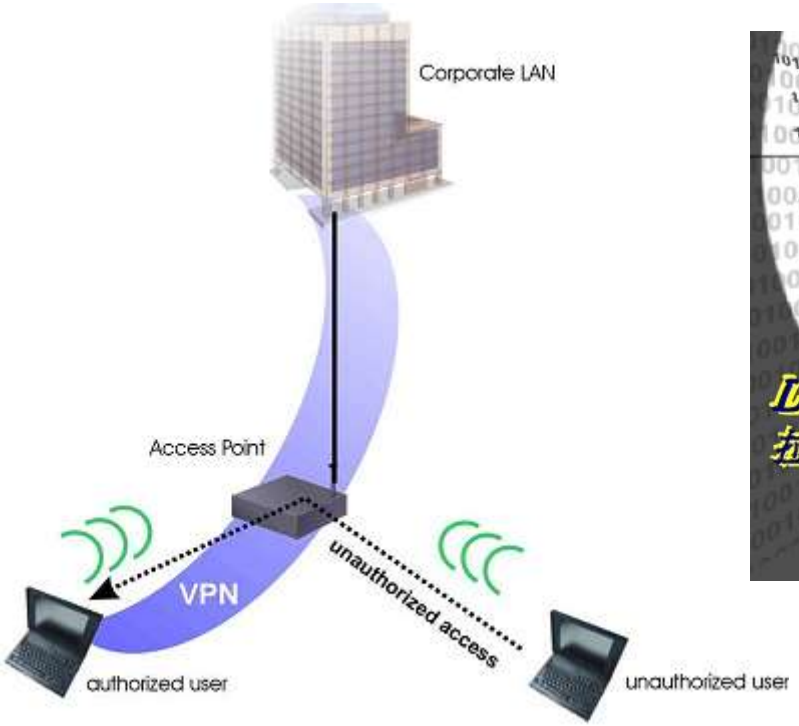
Altres atacs

- 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 inalàmbric 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.