



# Faran med Spyware

- eller: Vad alla andra vet om dig

Per Hellqvist  
Senior Security Specialist



***En falsk känsla av säkerhet  
är värre än en äkta känsla  
av osäkerhet***

# Vad det handlar om?

## Användarprofilering

### ***Def:***

***Metoder som används för att bestämma livsstilar, beteende och åsikter genom insamlandet av personlig information eller sannolikheten att en viss produkt inhandlas***

# Användarprofilering på internet

- 85% av kommersiella webbplatser samlar in uppgifter  
[Safeweb.com]
- Personlig information är den nya valutan för e-handel
- Genomsnittssamerikanen finns profilerad i mellan 25 till 100 databaser [FirstMonday.org]

# Typer av information

- PII : Personligt Identifierbar Information
  - Mest känsliga typen: personnamn, hemadress, personnummer, etc
- Icke-PII : All annan information som samlas in om en användare och som inte är direkt anknyttat till PII
  - Till exempel IP adresser (läs privacy statements)

# Personlig integritet - Privacy

*American Heritage Dictionary, Tredje upplagan,*  
“The state of being free from unsanctioned intrusion: a person’s right to privacy.”

*Oxford English Dictionary,*  
“The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion.”

# Nivåer av personlig integritet

- ***Din person***  
Bekymrad över din personliga integritet som person
- ***Ditt beteende***  
Oavsett om det rör sig om sexuellt, politiskt, religiöst eller shoppingbeteende
- ***Din personliga kommunikation***  
Rätten att kommunicera utan övervakning
- ***Integriteten av dina personliga data***  
Personliga data borde inte finnas tillgängliga för andra utan vidare

“You have zero privacy anyway. Get over it.”

Scott McNealy  
CEO, Sun Microsystems  
January 1999



# Processen

- Hur samlas personlig information in?
- Hur skapas användar profiler från personlig information?
- Hur används användarprofiler?

# Lågnivåprotokoll - TCP/IP

- DNS-servrar
  - Underhålls av ISP'er
  - Håller reda på namnen på servrar som användare försöker kontakta
- Routing
  - Den genomsnittliga internetanvändaren kan inte ändra hur IP paketen routas
- Ping-kommandon
  - Gör att vem som helst på internet kan se om en viss dator är påslagen och uppkopplad
  - (Personlig) brandvägg hindrar detta!

# Högnivåprotokoll – HTTP

- Osynliga länkar kombinerat med den information man får fram från webbläsaren etc används av annonsörer
  - T ex DoubleClick, 24/7 Media och Engage
- När man söker i en sökmotor innehåller URL'en orden du söker på
- Dessa sökord sänds vidare till annonsörer som väljer ut en lämplig banner

# Information som lämnas vid surfning (web chattering)

| <i>HTTP<br/>Var.</i>    | <i>Opera 3.50</i>                                         | <i>Netscape 4.0 Fr</i>                    | <i>Explorer 4.0 UK</i>                                                                                                                                     |
|-------------------------|-----------------------------------------------------------|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>GET</b>              | GET /index.html<br>HTTP/1.0                               | GET /index.html HTTP/1.0                  | GET /index.html<br>HTTP/1.0                                                                                                                                |
| <b>User-<br/>Agent:</b> | Mozilla/4.0(compatible;<br>Opera/3.0; Windows 95)<br>3.50 | Mozilla/4.04 [fr] (Win95; I<br>;Nav)      | Mozilla/4.0 (compatible;<br>MSIE 4.01; Windows<br>95)                                                                                                      |
| <b>Accept :</b>         | image/gif, image/x-<br>bitmap, image/jpeg, /              | Image/gif, image/x-<br>bitmap, image/jpeg | image/gif, image/x-<br>bitmap, image/jpeg,<br>image/pjpeg,<br>application/vnd.ms-<br>excel,<br>application/msword,<br>application/vnd.ms-<br>powerpoint, / |
| <b>Referer :</b>        |                                                           | Where.were.you/doc.htm                    | Where.were.you/doc.htm                                                                                                                                     |
| <b>Language</b>         |                                                           | Fr                                        | fr-be                                                                                                                                                      |

# Högnivåprotokoll – HTTP

## Cookies

- Cookies gör det möjligt att systematiskt sända en permanent och unik identifierare med varje förfrågan
- IP-adresser är en relativt svag identifierare
  - Kan gömmas av proxies
  - Allokeras dynamiskt för modemanvändare

# Cookiefil i Netscape

```
# HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This is a generated file! Do not edit.
# To delete cookies, use the Cookie Manager.

.traffic.ro TRUE / FALSE 2115295200 traffic_ranking 342a3defd0c1d68b258779262a4132b6
www.shockcounter.com FALSE /cgi-bin/ FALSE 1072768490 www.hidro.4t.com 1
.aftonbladet.se TRUE / FALSE 1293839999 RMID c354cce23f0054f0
.imrworldwide.com TRUE /cgi-bin FALSE 1232319604 IMRID
PwBU9MLAu7oAADpsAWU
as1.falkag.de FALSE / FALSE 1063374139 BSUID 5552ACA4
.admeta.com TRUE /public FALSE 1063144800 visitor%5Fid 9126516
.servedby.advertising.com TRUE / FALSE 1063371615 27585
_3f3a365f,,80590^98595_
.servedby.advertising.com TRUE / FALSE 1063371779 5012
_3f3a3703,,80590^98595_
.advertising.com TRUE / FALSE 1214666269 ACID
ee570010569862690001!
.2o7.net TRUE / FALSE 1215015080 s_vi_atamox7Ecaihem
[CS]v3|3F05A6DC00001EED-
A000A5300000001|3F05A6DB|3F05A6DC|3F05A726|1|2|0|0|QMMIx03x16x16NNNx17TXZKVTx5Cx5DPXx17ZVTx16JQVZRNxOx5Cx16x5DV
NWUVXx5Dx16x5DVNWUVXx5Dx17Zx5EP|QMMIx03x16x16NNNx17TXZKVTx5Cx5DPXx17ZVTx16JQVZRNxOx5Cx16x5DVNWUVXx5Dx16x5DVNWUVXx
5Dx17Zx5EP|[CE]
wdcs.trendmicro.com FALSE / FALSE 1372694991 WEBTRENDS_ID 195.84.204.226-
2997620208.29573702::2B09C76B2AA591EBE799088A8CD8A19A
www.krzr.com FALSE / FALSE 1088523184 CCIT_YEAR
195.84.204.226.308601056987184521
www.clearchannel.com FALSE / FALSE 1214667188 HSUSER
3X195.84.204.226X9778X1056987188X558
ads4.clearchannel.com FALSE / FALSE 2145803451 NGUserID a010acb-2304-
1056985332-5
www.clearchannel.com FALSE / FALSE 1214667188 u_krzr-fm
3X195.84.204.226X9778X1056987188X558
.google.com TRUE / FALSE 2147368052 PREF
ID=75f14173345d0f1:TM=1056986462:LM=1056986462:S=NMm8AXbv7uwrKYCX
```

# Cookies

- I sig inte ett problem
- Används för att spara inställningar du gjort etc
- En svaghet i IE gör det dock möjligt att hämta cookies från din dator

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-015.asp>

- Ett script läggs i en URL eller i ett html-formatterat mail

# Vanligt med ad-cookies?

- DoubleClick - 16.219
- BeFree – 3.257.795
- AvenueA – 666
  
- Det är lättare att hitta än att missa dem...

# Fuling: DoubleClick

- Double-Click :
  - Planerar att skapa en databas med användarprofiler som innehåller varje användares
    - ❖ Namn
    - ❖ Adress
    - ❖ Inköphistoria
    - ❖ Demografiska data
    - ❖ etc
  - Slår ihop sin databas med marknadsföraren Adacus direct

## Content of the DoubleClick database

*(Sources : interviews and documentation of DoubleClick - New York - June 1997)*

| Personal data                                                                                                                     | Comments                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| - IP address                                                                                                                      | Although dynamic, the IP address is composed of permanent data that is standardized and indexed at an international level and makes it possible to identify the network to which the user belongs, i.e. it is the Net address. DoubleClick's databases contain about 400,000 Net addresses. If the Net address cannot be found in DoubleClick's tables, the central system is set to send an automatic request to Inter-nic <sup>(11)</sup> |
| - Domain (e.g: at&t.net, microsoft.com, etc.)<br>- Country<br>- State (United States)<br>- Postcode<br>- SIC code (United States) | These five information items are revealed by the Net address. The domain name identifies the user's occupation (student, civil servant, etc.); the SIC code identifies the sector in which the company operates; it is collected from a third organization, is matched with the domain name and becomes a basic element of the DoubleClick data; e.g.: code 7372 = software package engineering                                             |
| - Job title and function within the company                                                                                       | This data is not yet available, but DoubleClick has announced that it will be in the near future.                                                                                                                                                                                                                                                                                                                                           |
| - Size and turnover of the company                                                                                                | This is data concerning a business user; the information is collected by DoubleClick from external sources and stored in the database                                                                                                                                                                                                                                                                                                       |
| - Type of browser used<br>- Operating system<br>- Version number<br>- Service provider                                            | These four information items are contained in the header of an HTTP request. They are collected once and for all the first time a user is identified and recorded in the DoubleClick databases                                                                                                                                                                                                                                              |
| - Identification number                                                                                                           | This number is unique and is assigned by the DoubleClick databases as soon as a user who visits one of the Websites of the DoubleClick network and accepts a <i>cookie</i> is identified                                                                                                                                                                                                                                                    |
| - Referencing of browsing activities                                                                                              | Collection and analysis of the sites visited by the user: information, sports, weather forecasts, finance etc. Determination of the keywords contained in the pages displayed if relevant; session times and days of the week on which they occur                                                                                                                                                                                           |

# Fler källor till personlig information

- Nyhetsgrupper:
  - Meddelanden som sänts finns tillgängliga i flera år
    - ❖ Speciella sökprogram finns för att profilera avsändare
  - Mumma för datamining & datawarehousing
  
- ...och hackare!
  - Perfekt underlag för Social Engineering

# Web Browser Extensions

- The Privacy Foundation laddade ned 16 tilläggsprogram till Internet Explorer och övervakade deras funktion
- Inte en enda visade för användaren allt de gjorde
- Över 50% sände iväg information som påverkar användarens integritet även om produkten i sig inte kräver det för att fungera

# Web Browser Extensions

## Fuling: RealJukeBox

- RealJukeBox gör att man kan spela CD-skivor, spela in musik till datorn (rippa till MP3)
- ...Vad den också gör är att övervaka vilken musik som spelas och sända informationen tillbaka till Real.com tillsammans med ett GUID som identifierar användaren som registrerade programmet

**Ja, ja, men kom till saken...!**

# Definitioner

## ■ **Spyware**

- Spyware är ett program som “sänder in” information om vad du gör
- Företaget som tar emot informationen är vanligen en tredjepart och inte tillverkaren/distributören av mjukvaran den ligger i

## ■ **Adware**

- En speciell typ av spyware som visar annonser
- Ligger ofta i “gratis” programvara

# Spyware (mer exakt definition)

- Mjukvara som samlar in information om en användare när han/hon “surfar” på nätet. Syftet är att spåra surfvanor för att bygga upp marknadsföringsprofiler. Spyware finns ofta i “gratisprogram” där licensavtalet (EULA, som många av oss inte läser alls) kanske nämner att information om dina vanor kommer att sändas tillbaka till företaget
- <http://www.netlingo.com/lookup.cfm?term=spyware>

# Problemet med Spyware

- Laddar ned annonser och slösar systemresurser
- Slöar ned systemet
- Gör saker som jag inte vill eller vet om
- Kraschar webbläsaren?
- Kraschar Windows?
- Om spywaret raderas kanske du inte kan surfa....
- Och värst av allt: kompromitterar din personliga integritet och mer... !

# Problemet med Spyware

- **Spyware är ett fristående program som installerar en del osäkra funktioner**
  - AutoInstall, AutoUpdate
  - Dörröppnare för elaka program?
- **Tunn linje mellan Spyware och trojaner**
  - Trojanen Idly samlar in systeminformation, dial-up inställningar och sänder dem till hackaren
  - (<http://securityresponse.symantec.com/avcenter/venc/data/trojan.idly.html>)
- **IT-avdelningen kan blockera domänerna till reklamföretagen**
  - Dyrt att underhålla
- **Slutanvändaren måste ta ett ansvar**

# Andra problem

## Trojaner, hackerverktyg och annat

- 1.898 st Remote Access Trojans (RAT) (1.195 (+703))
- 481 st Keyloggers (229 (+252))
- 542 st lösenordsstjälare (371(+171))
- 264 st Hackerverktyg (79(+185))
- 281 st DoS-verktyg (117 (+164))
- 595 st Destruktiva trojaner (441 (+154))
- 292 st Anti-protection tools (124 (+168))

Source: Joakim von Braun. Statistics based on 5.357 files, 2003-09-21 (3.752)

# Typiskt beteende

- Sänder in en lista över webbplatser du besökt
- Övervakar det du gör och sänder popup reklam baserat på vilka typer av webbplatser du besöker
  - “Köp toner!” ploppar upp när du skriver ut
- Uppringare för porr etc
- Sänder felmeddelanden från IE till reklamplatser

# Ökande problem

- När en skola i Australien gjorde en genomgång fann man över 4000 installationer på 1250 datorer
- ISP'n EarthLink ränkar med att 40-50% av deras användare har spyware installerat

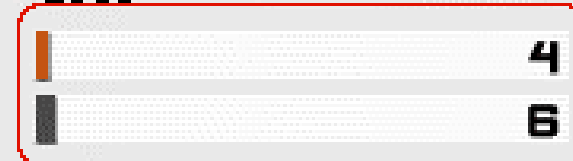
## GROWTH SPURT

ACCORDING TO SECURITY SOFTWARE FIRM PEST PATROL, THE NUMBER OF ADWARE AND SPYWARE PROGRAMS SURGED IN 2002.

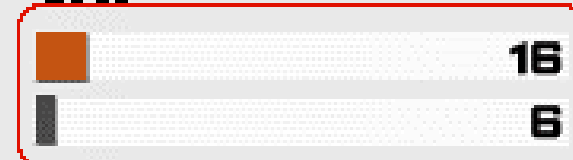
■ SPYWARE

■ ADWARE

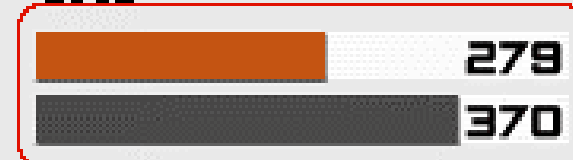
2000



2001



2002



STATISTICS FROM PEST PATROL REPORT DATED FEB. 19, 2003. NOTE: DEFINITIONS OF "ADWARE" AND "SPYWARE" ARE NOT STANDARD. PEST PATROL'S CATEGORIZATIONS MAY NOT MATCH OTHERS.

# Spyware

- Hur får man in det?
  - Man laddar ned något program som innehåller spyware
    - ❖ T ex Kazaa eller Hotbar
  - Man besöker en webbplats som placerade en spyware-cookie i din dator
  - Man installerar det (av misstag) genom att klicka “fel” på en popup på en webbplats
  - Det installerar sig själv på din dator utan din vetskap

# Program med Spyware

## (Ofullständig lista)

### 1x

100% Word Search Free®  
123Search®  
2MinuteWarning®  
3d Anarchy®  
3D Frog Man Demo®  
3D Maze Man Demo®  
3D-FTP®  
3rd block®

### A

Abe's FTP Client®  
Abe's Image Viewer®  
Abe's MP3 Finder®  
Abe's Picture Finder®  
Abe's SMB Client®  
Absolute Yukon Solitaire®  
Access Diver III®  
Aces and Kings Solitaire®  
Acorn Email®  
AcqURL®  
ActionOutline Light 1.6®  
Active 'Net®  
AddAce®  
Add URL®  
Add/Remove  
  Plus!®Add/Remove  
  Plus!®  
Address Rover 98®  
Admiral VirusScanner®

Advanced Call Center®  
Advanced Maillist Verify®  
AdWizard®  
Alchemist Demo®  
Alive and Kicking®  
alphaScape QuickPaste®  
Apload Notify®  
ASP1-A3®

### Auction Explorer®

Aureate Group Mail®  
Aureate SpamKiller®  
AutoFTP PRO®  
AutoWeb®  
AxeICD®

### B

Balloon Pop Demo®  
Banner Crafter®  
Beatle®  
Binary Boy®  
BinaryVortex®  
Bingo Demo®  
Bingo Master Demo®  
Blast Thru Demo®  
Blue Engine®  
BookSmith : Original®  
buddyPhone 2®  
Business Letter Punch®

### C

Calypso E-mail®  
CamGrab®  
Capture Express 2000®  
Cascoly Screensaver®  
CDDB-Reader®  
CDMaster32®  
ChanStat®  
Charity Banner®  
Chat PicPluck®  
Cheat Machine®  
Check & Get®  
Check4New®  
Chinese Checkers  
Demo®  
ChinMail®  
Clabra clipboard  
viewer®  
Classic Peg Solitaire®  
CoffeeCup Free  
HTML®  
ComTry Music  
Downloader®  
Connect ?®  
Crazy Drake Demo®  
Crazy Puzzle Demo®  
CrushPop®  
Crystal FTP®  
CSE HTML Validator  
Lite®  
CS Telnet®  
Cursor Maker®  
CuteFTP®  
CuteFTP 3.0®  
CuteFTP 3.0 beta®  
CuteFTP/Tripod®  
CuteMX®  
CutePage®

### D

Danzig Pref Engine®  
DateTime®  
DB to HTML Express®  
Debt Relief®  
Delphi Component Test®  
Delphi Tester®  
Develop Critical Thinking Skills®  
Dialer 2000®  
DigiBand NewsWatch®  
DigiCams - WebCam Viewer®  
Digital Postman®  
Digital Postman®  
DirectUpdate®  
DL-Mail Pro 2000®  
DNScape®  
Doorbell 1.18®  
dotCool Builder®  
Download Minder 1.5®  
Download Wonder®  
DownLoader v.1.1®  
Dweebs Demo®  
Dwyco Video Conferencing®

### E

EconForecast®  
EasySeeker®  
EmmaSoft ChatCat®  
EmmaSoft dBrow®  
EmmaSoft KeepLan®  
EmmaSoft Soundz®  
eMNGma®  
EnvoyMail®  
Essay-Punch®  
Extreme Animals Demo®  
Extreme Bugs Demo®  
Extreme Dinosaurs Demo®  
Extreme Orchids Demo®  
EZ-Forms FREE®

### F

File Mag-Net®  
File Sniffer®  
FileSplit®  
FlexSpex®  
Folder Guard Jr.®  
FourTimes®  
Free Picture Harvester®  
Free Solitaire®  
Free Solitaire®  
Free Spades®  
Free Submitter Pro®  
FreeImageEditor®  
FreeIRC®  
FreeNotePad®  
FreeSite®  
FreeWebBrowser®  
FreeWebMail®  
FreeZip!®  
FTPEDITOR®

### G

Galactic Invasion Demo®  
Galaxy of 3D TetriMania Demo®  
Gardener Demo®  
Garret Demo®  
GetRight®  
Glowing Bugs Demo®  
Go!Zilla®  
Go!Zilla WebAttack®  
GovernMail®  
Grafula®  
Grammar Fitness Suite®  
Gunther's PasswordSentry®  
Gypsee®

# Program med Spyware

## H

HangWeb®  
hesci Private Label®  
Hexx Wars II®  
Home Buyer's Calculator Suite®  
HTML Translator®  
HTTP Proxy-Spy®  
Huey v1.8 Color Picker®

## I

Iban Technologies IP Tools 3.1®  
Idle GimmiP®  
Idle GimmiP®  
iFind Graphics®  
Image Carousel®  
Image Site Grabber®  
imageN®  
InboxSpecialist®  
Infinite Patience®  
InfoBlast®  
InnovaClub®  
InstallZIP®  
Intergalactic Exterminator Demo®  
Internet Tree®  
Internetrix®  
InterWebWord Companion®  
IPLAY®  
iSolitaire®

IVOX® IVOX ICQ®

## J

JetCar®  
JFK Research®  
jIRC®  
JOC Email Checker®  
JOC Web Finder®  
JOC Web Spider®  
K  
KVT Diplom®  
L  
LapLink FTP®  
Lexicon Demo®  
Link Crafter®  
LineSoft Download®  
LivePaper®  
Loan Calculator Plus®  
LOL Chat®  
Ludo Safari Demo®  
M  
Mahjongg Master 2 Demo®  
MailAlert®  
Mail Them®  
Meracl FontMap®  
Meracl ImageMap Generator®  
Midnight Oil Solitaire®  
MidWaviPro®  
Mini Golf Demo®

## MirNik Internet Finder®

More Space 99®  
MouseAssist®  
MP3 Album Finder®  
MP3 Album Finder®  
MP3 Fiend®  
MP3 Grouppie®  
MP3 Mag-Net®  
MP3 Renamer®  
Mp3 Stream Recorder®  
MP3INFO-Editor®  
Mr. Cool®  
MSi-Clip®  
MultiSender®  
Music Genie®  
MX Inspector BIG AD®  
My Genie Patriots®  
My Genie SE®  
My GetRight®  
N  
NeatFTP®  
Nebula Fighter Demo®  
Net CB®  
Net Scan 2000®  
Net Vampire®  
Net-A-Car Feature Car ScreenSaver®  
NetAnts®  
NetBoard®  
Netbus Pro 2.10®  
NetCaptor 5.0®

## Netman Downloader®

NetNak®  
NetScoopFinance®  
NetSuck 3.10.5®  
NetTime Thingy®  
Network Assistant®  
NeuroStock®  
NewsBin®  
News-Lynx®  
NewsShark®  
NewsWire®  
NfoNak®  
NotePads+®  
Notificator 1.0b®  
O  
Octopus®  
Of The Day Quizzer®  
Oxide Demo®  
P  
Paragraph Punch®  
Patriot Slots®  
Pattern Book®  
PCDJ PHAT®  
People Seek 98®  
Personal Auction Track®  
Personal Search Agent®  
Personal Stock Monitor SE®  
Photocopier®  
Photocopier®  
PicPluck®  
Pictures In News®  
Ping Thingy®  
PingMaster®  
PKZip®  
Planet.Billboard®  
Planet.MP3Find®  
PMS®  
Powerzip 2000 Lite®  
ProtectX 3®  
ProxyChecker®  
Puzzle Master Demo®

## Q

QuadSucker/Web®  
Quadzle Puzzles®  
QuikLink Autobot®  
QuikLink Explorer®  
QuikLink Explorer Gold Edition®  
QuoteWatch®  
QuoTracker®  
QWallet®  
R  
RahJongg Demo®  
Raptor Call of the Shadows Demo®  
Real Estate Web Site Creator®  
Recipe Review®  
ReGet®  
ReGet 1.6®  
Resume Detective®  
RingSurf®  
RoboCam 1.10®  
Rosemary's Weird Web World®  
RubberDuck H30+®  
S  
SaberQuest Page Burner®  
SafeNet Mail®  
SBJV®  
SBWcc®  
Scout's Game®  
ScreenFIRE®  
ScreenFIRE - FileKing®  
ScreenFlavors®  
Sea Battle®  
Shakespeare Punch®  
Shizzam®  
ShortKeys Lite®  
Simple Submit®  
SimpleFind®  
SimpleSubmit v1.0®  
Simplicity Personal Organizer®  
Site Select®  
SK-111®

# Program med Spyware

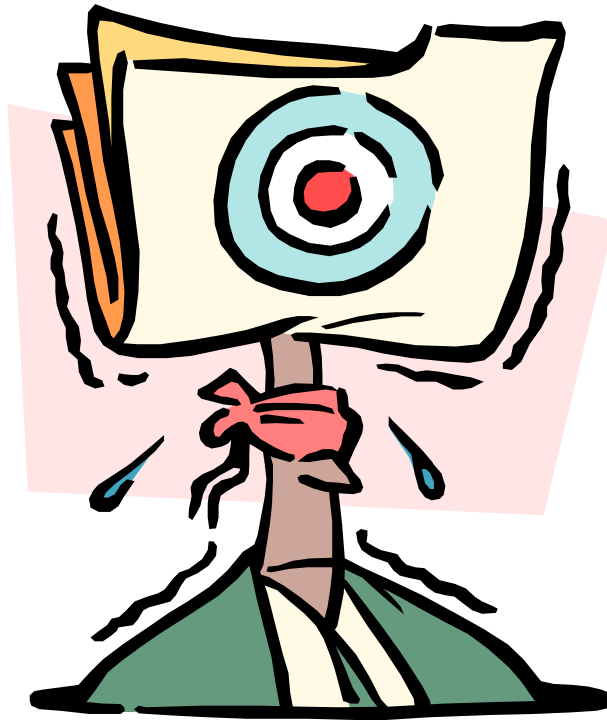
SL4 Historical Montage®  
Smart 'n Sticky®  
SmartBoard 200 FREE Edition®  
SmartDoc 3.0®  
SmartSum calculator®  
Sonic Mail®  
SonicMail®  
Sound Agent®  
Space Central Screen Saver®  
Speedy Eggbert Demo®  
Splash! Siterave®  
SSScanner®  
SSSiter®  
SSSpider®  
StartDrive®  
Star Miner Demo®  
Static FTP®  
StayOn Pro®  
StockBrowser®  
Stock Profit Spread Calculator 32®  
Subscriber®  
SunEdit 2K®  
Superball Challenge Demo®  
SuperIDE®  
Surf Saver®  
Sweep®  
SweepsWinner®  
System Agent®

T  
Tagger®  
TetriMania Master Demo®  
Text Transmogrifier®  
The Mapper®  
TheNet®  
TI-FindMail®  
TIFNY®  
Time Zone Converter®  
Tools 3.1®  
Total Finger®  
Total Whois®  
Tracking The Eye®  
Trade Site Creator®  
Trade Trakker®  
Tray Note Plus®  
TS-Image Mapper®  
Tunnel Blaster Demo®  
TWinExplorer Standard®  
TypeWriter 1.0®  
U  
ulCE®  
UK Phone Codes®

V  
Vagabond's Realm®  
VeriMP3®  
Vertigo QSearch®  
Virtual Access®  
Visual Cyberadio®  
Visual Surfer®  
VOG Backgammon Main®  
VOG Backgammon Table®  
VOG Chess Main®  
VOG Chess Table®  
VOG Reversi Main®  
VOG Reversi Table®  
VOG Shell®  
VOG Shell History®  
W  
W3Filer®  
War Demo®  
Web-Cam VCR®  
Web Coupon®  
Web Page Authoring Software®  
Web Registrant PRO®  
Web Resume®  
WebStripper®  
Web SurFACE®  
WEB2SMS®  
WebCamVCR®  
WebCopier®  
Web-N-Force®  
WebSaver®  
Website Manager®  
WebStripper®  
WebType®  
Whitehouse Mambo Parody®  
WhizFolders Organizer®  
Whois®  
Whols Thingy®

Win A Lotto®  
WinEdit 2000®  
Word+®  
Word Connect Demo®  
Word Search Mania Demo®  
Wordwright®  
WorldChat Client®  
Worm®  
Writing about Reading®  
Writing for Business®

# Ett par exempel



# WildTangent

## "Visualization for Media Players"

- Det officiella syftet är att sända annonser till datorn
- Egentligen hämtar den uppgift om efternamn, adress, telefonnummer, e-post, systemkonfiguration, CPU hastighet, DirectX-version, hur många gånger du startat vissa applikationer samt hur länge du använt produkten
- Hämtar ned och installerar program på datorn
- Läger in minst 625 olika objekt på datorn



# Kazaa Media Desktop

- Nedladdad 214 miljoner gånger...
- Läger in 79 olika objekt
- "Kazaa Media Desktop contains banner advertising and the option to install other third party applications in order to remain free to the user."



# BargainBuddy

- Ett Browser Helper Object som övervakar vilka webbplatser du besöker och vad du söker efter
- Jämför detta med en inbyggd lista
- Finns ditt “intresse” på listan visas passande reklam från DoubleClick
- Listan uppdateras utan att du vet om det från [adp.ikena.com](http://adp.ikena.com).
- DoubleClick spårar sedan ditt surfande med Cookies

# DN.Börs

&lt;Annon&gt;

**FREE MEMBERSHIP NO CREDIT CARD  
NEEDED!**

CLICK HERE!

Hem DN Börs Nyheter Till DN Om DN Börs Hjälp Kontakt

Börsen - 0,5%



## Min Portfölj

## Börsen nu

## Aktier

## Börsen

## Sök i Börsen

## NGM-listan

## Inofficiella

## Fonder (ny)

## Index

## Råvaror

## Obligationer

## Optioner

## Räntor

## Valutor

&lt;Annon&gt;

**FREE  
MEMBERSHIP  
NO  
CREDIT  
CARD  
NEEDED!  
CLICK  
HERE!**

Fredag 12 oktober 2001, 14:10

15 minuters fördröjning

Välkommen till  
**DN.Börs**



Kommentar Bolagsrapporter Börser Länkar Ordlista

## SENASTE NYTT FRÅN DN EKONOMI

- Aderas dotterbolag i konkurs  
[011012 13:33]
- Hackare försökte sig på utpressning  
[011012 13:25]
- Lufthansas vd spår utslagning inom flyget  
[011012 13:07]
- Saab justerar ner prognosen  
[011012 12:20]
- ABB får kinesisk 3,8 miljardorder  
[011012 12:15]
- SCB: Sparandet minskade  
[011012 11:37]
- Skadestånd mot mäklare förhandlas separat  
[011012 11:26]
- Medling inför journalistavtal  
[011012 10:56]

► Fler nyheter

## Svenska företags

## PRESSMEDDELANDEN

► Waymaker News

## fondskolan

► Gå i

DN:s

fondskola.



## Aktiesökning

Skriv in en aktiesökning, eller flera  
separerade med komma

Sök

SX All-Share

OMX

VA Total index



## Marknaden

|                           | +/ -          | Senast        |
|---------------------------|---------------|---------------|
| Stockholm All-Share       | - 0,46        | 212,78        |
| OMX (Realtid)             | - 0,39        | 759,82        |
| Räntor 90 dagar           | - 0,02        | 3,71          |
| Euro                      | 0,01          | 9,52          |
| Dollar                    | - 0,04        | 10,53         |
| <b>Vinnare A-listan</b>   | <b>+/ - %</b> | <b>Senast</b> |
| Lindex                    | 7,11          | 113,00        |
| Autoliv Inc               | 4,40          | 178,00        |
| Consilium B               | 3,67          | 32,60         |
| Scribona B                | 3,00          | 10,30         |
| Stora Enso A              | 2,95          | 126,00        |
| <b>Förlorare A-listan</b> | <b>+/ - %</b> | <b>Senast</b> |
| Scribona A                | - 7,18        | 9,50          |
| Cardo                     | - 5,90        | 159,00        |
| Haldex                    | - 3,61        | 80,50         |
| Höganäs B                 | - 3,17        | 154,00        |
| SSAB B                    | - 3,03        | 80,00         |

&lt;Annon&gt;

**FREE  
MEMBERSHIP  
NO CREDIT  
CARD  
NEEDED!  
CLICK  
HERE!**

\*\*\*\*\* DOV



ALANIS MORISSETTE

# Andra datainsamlare

- RedSherriff
  - Javascript som ligger på en del webbplatser
  - Skickar information om hur du använder internet
  - Hur lång tid sidan tog att ladda
  - Hur länge du stannade på sidan, etc
- CensorWare
  - Samlar in information om barns surfvanor
- RealJukebox
  - Håller koll på vilken musik du lyssnar på och sänder det tillbaka till Real Networks

# Och förstås ... Gator

**Gator.com - Home - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail News Groups

Address <http://www.gator.com/> Go

**"YOU'LL NEVER HAVE TO FILL IN ANOTHER WEB FORM AGAIN."**  
-THE NEW YORK POST

The Gator Corporation

**FREE DOWNLOAD** CLICK HERE

**SEE PRODUCT DEMO** CLICK HERE

HOME ADVERTISE WITH US COMPANY INFO ABOUT GATOR SUPPORT CENTER CONTACT US

**GATOR<sup>SM</sup> eWALLET. THE SMART ONLINE COMPANION.**

- ▶ Fills in FORMS with no typing!
- ▶ Remembers PASSWORDS automatically.
- ▶ Protects and encrypts your data on YOUR computer.
- ▶ The Gator eWallet is ad-supported software. It is part of the Gator Advertising and Information Network ([GAIN](#)), which helps keep software free by delivering messages based on the sites you view.

**Order Information**

Fill out and submit the following form, making sure to enter information. Your order will be acknowledged via email.

**Credit Card Information/Shipping Information**

First Name: Brian  
Last Name: Martin  
Address (line 1): 124 South Park Dr.  
Address (line 2):  
City: Menlo Park  
State: CA  
Zip: 94025-1426  
Phone: 650-888-8888

Shipping: Work  
Address: 124 South Park Drive  
Suite 300  
Menlo Park, CA 94025

Shipping Phone: 124 South Park Drive  
Card: Yes  
Card Number: 1234567890123456  
Expiry: 01/2000 - 12/2001  
Bill To: Home address

☒ Visa ☐ Mastercard ☐ American Express

Card Number: 1234567890123456

I would prefer our transaction by: ☒ email ☐ fax

Order Reset

**We don't know who our users are...**

TGC does not know the identity of GAIN-Supported Software users. We do not transmit to our servers personally identifiable information like email addresses, last name, street addresses, or phone numbers. Nor do we have any other sensitive or personal financial information, such as credit card numbers, login IDs, passwords or bank account numbers. Any such information entered into any TGC GAIN-Supported Software application (such as the Gator<sup>SM</sup> eWallet) will remain on the personal computer upon which it was entered, and will not be sent to our servers.

**Here's what we do know...**

While we don't know the identity of GAIN-Supported Software users, the GAIN AdServer and TGC does anonymously collect and use the following kinds of information:

- Some of the Web pages viewed
- The amount of time spent at some Web sites
- Response to the ads displayed
- Standard web log information (excluding IP Addresses) and system settings
- What software is on the personal computer
- First name, country, and five digit ZIP code
- Non-personally identifiable information on Web pages and forms
- GAIN-Supported Software usage characteristics and preferences

We associate such information with a particular personal computer through a randomly generated Anonymous ID number and use it to accomplish the following:

- Enable the functionality provided in TGC GAIN-Supported Software applications (for example, when to offer help filling in a form or when to reset the personal computer's clock to the accurate time)
- Select and deliver installation files for optional new software



- Deliver ads and informational messages to a computer screen on behalf of advertisers who may be competitors of the Web pages viewed by a user.

Any information provided to any TGC employees or contractors, such as our technical support department, may be stored on our servers in archives of our support and customer service communications. This information, however, will not be associated with the information we may store and use listed above. <http://www.gatorcorporation.com/help/psdocs/datause.html>, incorporated herein by reference, provides a more detailed description of the information collected by TGC and how it is used.

We share anonymous aggregate information about what Web pages users view on the Internet. For example, we might tell a merchant that we have 50,000 users who buy books. We do not disclose information associated with any individual user to that merchant.

We sometimes use third party contractors who may be given access to any information we have so they may perform tasks that might otherwise be done by our employees. These contractors, however, have no rights to use such information for purposes other than those described herein; and they are subject to the same restrictions as our employees. In the event that TGC merges with another company, transfers or sells substantially all of its assets or capital stock to a third party, all collected information would be included in the merger, transfer or sale and that company would be bound by these Terms and Conditions just as we are bound today.

If legally required to do so, we will disclose to a third party any information we have.

#### **Distribution of GAIN<sup>SM</sup>-Supported Software and the GAIN<sup>SM</sup> AdServer.**

All GAIN-Supported Software comes with the GAIN AdServer. The distribution of GAIN-Supported Software may occur in several different ways including: a) by downloading software from a Web site; b) by clicking to download software from online ads (patent-pending); and c) through trial programs in which GAIN-Supported Software are included as an "opt-out" option with other software.

# Innehållet i en "normal" cookie

id

224404107

ads.gorillanation.com/

1024

194832768

30859217

1991443872

29569443

\*

# Innehållet i en cookie från Gator

GatorWebPdpCookie\_WUID

P0oNfAr7CDkAADmzCzY

gator.com/

1024

3499419136

29596209

3744441856

29584139

\*

GatorWebPdpCookie\_PluginTimer

1052116051

gator.com/

1600

4048875904

30295801

970013088

29561547

\*

GatorWebPdpCookie\_MSG

28%3A2%3A1%3A3ee85f7e%7C86%3A3%3A1%3A3f27926b%7C224%3A3%3A8%3A3f320f65%7C87%3A3%3A1%3A3f4a0d7c%7C88%3A3%3A1%3A3f4a0d83%7C89%3A3%3A1%3A3f4a0d8f%7C90%3A3%3A1%3A3f4a0d96

gator.com/

1024

3759419136

29596209

4004811856

29584139

\*

GatorWebPdpCookie\_PLCMNT

182%3A22%3A1%3A3ee85f7e%7C220%3A88%3A1%3A3f320f65%7C78%3A44%3A5%3A3f4a0d96

gator.com/

1024

3759419136

29596209

4005011856

29584139

\*

# Vad kan man göra åt problemet?

## Logiskt

- Läs EULA (licensavtalet)
- Fyll inte i korrekta uppgifter om det inte är *absolut* nödvändigt
- Fyll inte i en massa uppgifter i t ex Internet Explorer
- Svara *aldrig* på spam
- Klicka *nej* på popup-rutor
- Håll koll på Cookies

# Vad kan man göra åt problemet

## Logiskt (forts)

- Undvik att installera “gratisprogram”
- Implementera en policy som säger att användare inte får installera vad som helst på datorn
- Uppdatera antivirusprogrammet
- Stäng portar i brandväggen som inte behövs
  - Både ingående och utgående...

# Vad kan man göra åt problemet?

## Logiskt (forts)

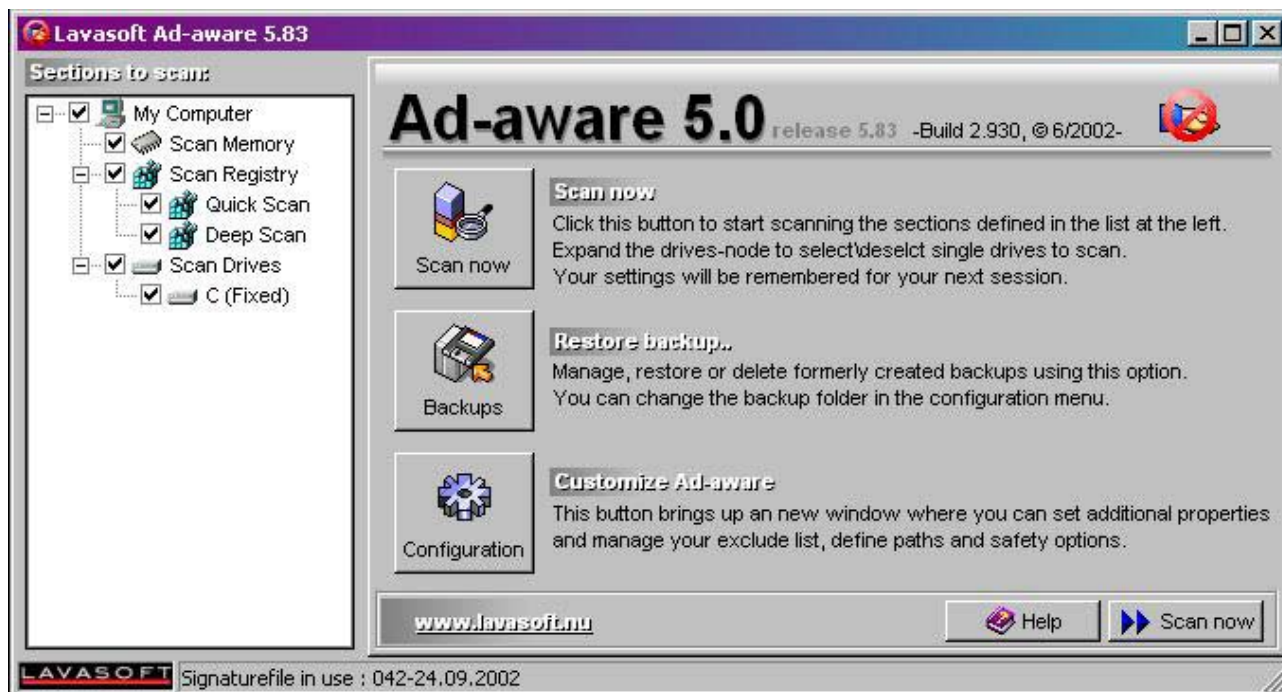
- Om allt annat falerar...
  - Använd en sniffer för att se vad som sänds och tas emot av spyware
  - Editera *Host*-filen och lägg in följande för varje server
    - ❖ 127.0.0.1      ad.server.com

# Vad kan man göra åt problemet?

## Lavasoft Ad-Aware

[www.lavasoft.de/support/download](http://www.lavasoft.de/support/download)

- Lavasoft är störst i branschen på att leverera “anti-Trackware”



# Vad kan man göra åt problemet?

## Spybot Search & Destroy

[www.cheatengamers.com/spybot/index.htm](http://www.cheatengamers.com/spybot/index.htm)

- Spybot-S&D letar upp och tar bort olika typer av spyware från datorn
- I version 1.2 finns också en slags “immunisering”, som kan blockera många spyware innan de installeras på datorn

# Vad kan man göra åt problemet?

## PestPatrol

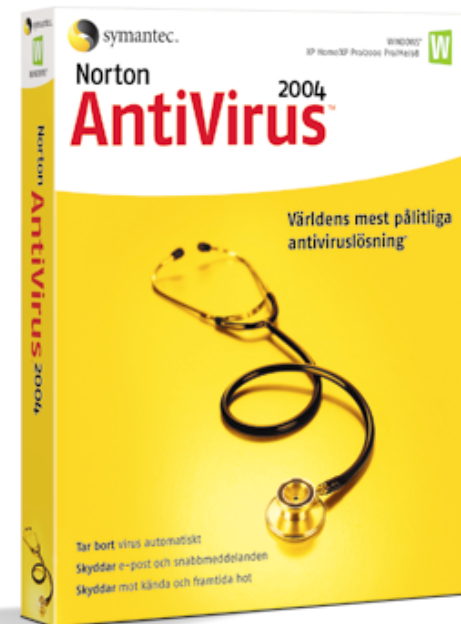
- <http://www.pestpatrol.com>
- Letar efter allt som inte är "virus":
  - Trojanska hästar, vissa cookies, denial-of-service zombies, hackerverktyg, spyware och adware

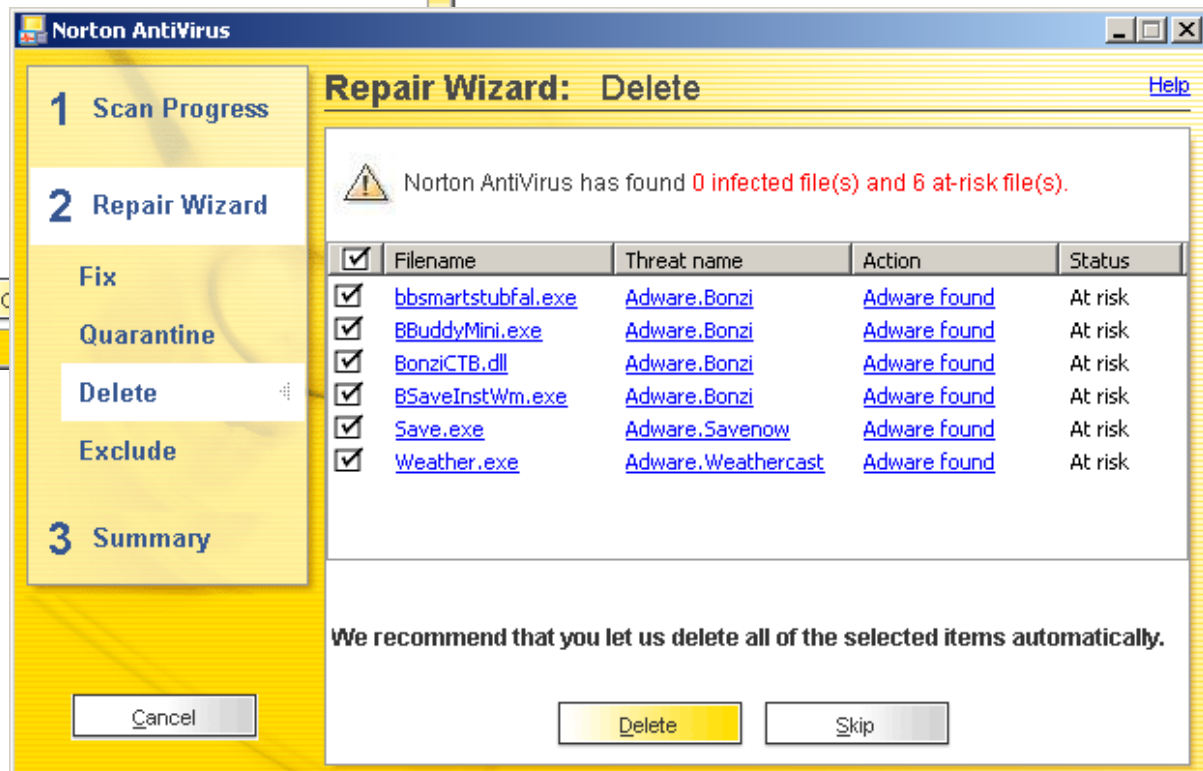
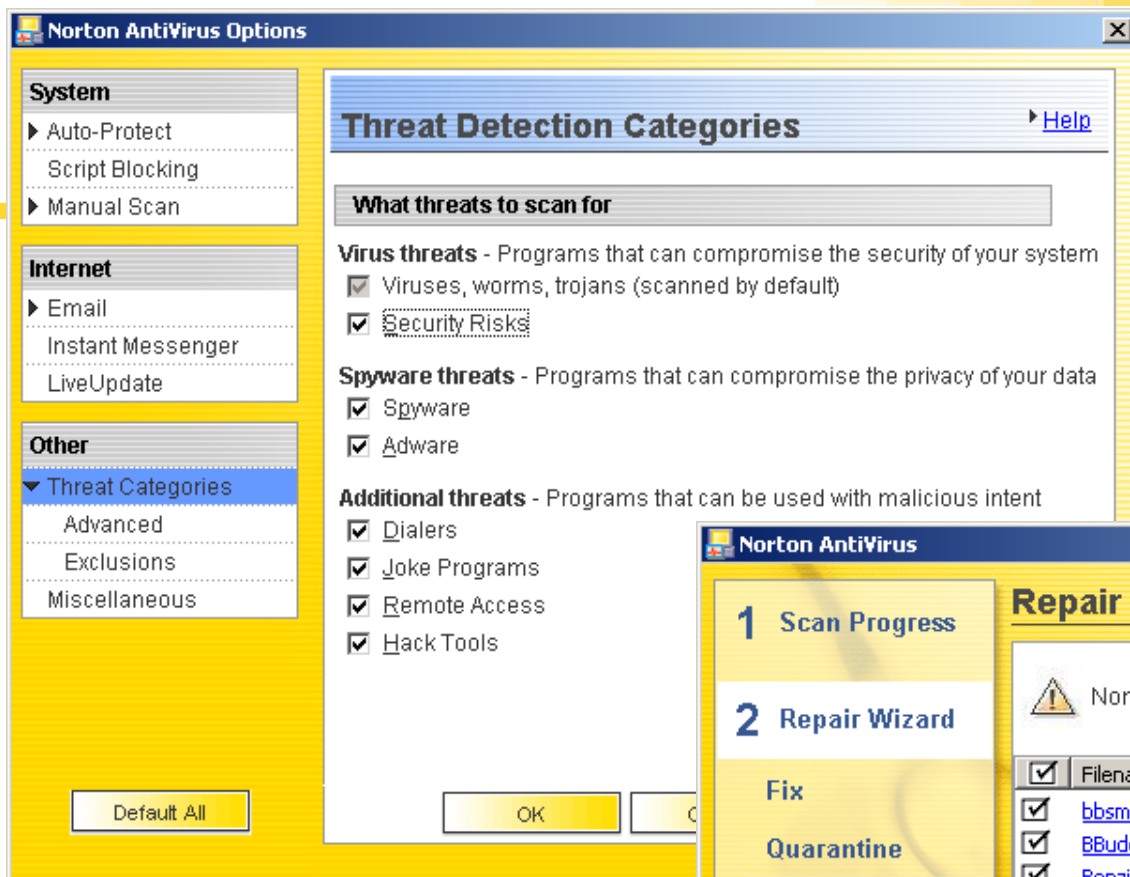


# Vad kan man göra åt problemet?

## Norton AntiVirus 2004

- **Förbättrad teknik för identifiering av hot**
- Norton AntiVirus tidigare skydd mot virus, maskar och trojaner har utökats och skyddar nu även mot spionprogram, reklamprogram, program som loggar tangenttryckningar och vissa program som används av hackare för att
  - påverka säkerheten i systemet
  - spionera på personlig information
  - spåra vad du gör på Internet





# Frågor?



