HAY UN ESPIA EN TU ORDENADOR

En el mundo actual, la incidencia de Internet en la sociedad se hace cada vez más palpable. Cada vez más y más personas usan Internet, prácticamente todo el mundo lo ha usado alguna vez.

Este uso cada vez mayor de Internet ha creado un nuevo tipo de espionaje: el espionaje informático y aunque parezca imposible cualquiera puede ser espiado... en su propia casa... en su propio ordenador.

Entre los usuarios de Internet es común el uso de programas para realizar downloads, tales como el Go!Zilla o el GetRight, de gran utilidad, no se puede negar, pero lo que los usuarios no saben es que además son unos grandes espías; ya que al instalarlos, también se instala un programa llamado "AureateSpy" que no pierde de vista tus actividades en Internet y envían un informe a Aureate cada vez que abres tu navegador.

Go!Zilla y GetRight son dos ejemplos, pero la lista de programas que instalan el AureateSpy es enorme, de momento los programas que se conocen que instalan el AureateSpy puedes verlos en la tabla adjunta.

Un total de ¡¡¡280!!! programas conocidos.

Conoce a tu enemigo... y tendrás media guerra ganada.

El AureateSpy coloca los ficheros siguientes en las máquinas Windows (no se sabe con certeza, pero se sospecha que también puede afectar a las máquinas de Macintosh o de Linux).

Los ficheros instalados por el AureateSpy (aunque puede que no se instalen todos los de la lista) son:

adimage.dll	advert.dll
advpack.dll	amcis.dll
amcis2.dll	amcompat.tlb
amstream.dll	anadsc.ocx
anadscb.ocx	htmdeng.exe
ipcclient.dll	msipcsv.exe
tfde.dll	

Aquí está un examen de las funciones de algunas de las DLL's de las que AureateSpy hace uso:

ADVERT.DLL

Esta DLL crea una ventana ocultada cada vez que abres tu navegador. Esta crea y envía 4 paginas de información a los servidores de Aureate usando el puerto 1749 de tu sistema, estas paginas incluyen:

1. Tu nombre según como conste en el registro del sistema (no el nombre instalado con los programas).
2. Tu dirección IP.
3. Las DNS de tu dirección (les dice qué ISP y área del país donde te encuentras).
4. Un listado de Todo el software instalado que se muestra en el registro.

- 123Search
- 3d Anarchy
- 3D-FTP
- 3rd block
- Abe's FTP Client
- Abe's Image Viewer
- Abe's MP3 Finder
- Abe's Picture Finder
- Abe's SMB Client
- Access Diver III
- Acorn Email
- AcqURL
- ActionOutline Light 1.6
- Active 'Net
- Add URL
- Add/Remove Plus!
- Address Rover 98
- Admiral VirusScanner
- Advanced Call Center
- Advanced Maillist Verify
- AdWizard
- Alive and Kicking
- alphaScape QuickPaste
- ASP1-A3
- Auction Explorer
- Aureate Group Mail
- Aureate SpamKiller
- AutoFTP PRO
- AutoWeb
- AxelCD
- Beatle
- Binary Boy
- BinaryVortex
- Blue Engine
- BookSmith : Original
- buddyPhone 2
- Calypso E-mail
- CamGrab
- Capture Express 2000
- Cascoly Screensaver
- CDDB-Reader
- CDMaster32
- ChanStat
- Charity Banner
- Cheat Machine
- Check4New
- ChinMail
- Clabra clipboard viewer
- Classic Peg Solitaire
- ComTry Music Downloader
- Crystal FTP
- CSE HTML Validator Lite
- CuteFTP 3.0
- CuteFTP 3.0
- CuteFTP/Tripod
- CuteMX
- CutePage
- Danzig Pref Engine
- DateTime
- Delphi Component Test
- Delphi Tester
- Dialer 2000
- DigiBand NewsWatch
- DigiCams - The WebCam Viewer
- Digital Postman
- DirectUpdate
- DL-Mail Pro 2000
- DNScape
- Doorbell 1.18
- Download Minder 1.5
- Download Wonder
- DownLoader v.1.1
- Dwyco Video Conferencing
- EasySeeker
- EmmaSoft ChatCat
- EmmaSoft dBrow
- EmmaSoft KeepLan
- EmmaSoft Soundz
- EnvoyMail
- EZ-Forms FREE
- File Mag-Net
- FileSplit
- Folder Guard Jr.
- FourTimes
- Free Picture Harvester
- Free Solitaire
- Free Spades
- Free Submitter Pro
- FreeImageEditor
- FreeIRC
- FreeNotePad
- FreeSite
- FreeWebNavegador
- FreeWebMail
- FreeZip!
- FTPEditor
- GetRight
- Go!Zilla
- Go!Zilla WebAttack
- GovernMail
- Grafula
- Gunther's PasswordSentry
- HangWeb
- hesci Private Label
- HTML Translator
- HTTPProxy-Spy
- Huey v1.8 Color Picker
- Iban Technologies IP Tools 3.1
- Idyle GimmIP
- Idyle GimmIP
- iFind Graphics
- imageN
- Infinite Patience
- InfoBlast
- InnovaClub
- InstallZIP
- Internet Tree
- Internetrix
- InterWebWord Companion
- JetCar
- JFK Research
- jIRC

- JOC Email Checker
- JOC Web Finder
- JOC Web Spider
- KVT Diplom
- LapLink FTP
- LineSoft Download
- LOL Chat
- LOL Chat
- Mail Them
- Meracl FontMap
- Meracl ImageMap Generator
- Midnight Oil Solitaire
- MirNik Internet Finder
- More Space 99
- MouseAssist
- MP3 Album Finder
- MP3 Fiend
- MP3 Grouppie
- MP3 Mag-Net
- MP3 Renamer
- Mp3 Stream Recorder
- MP3INFO-Editor
- MultiSender
- Music Genie
- MX Inspector BIG AD
- My Genie Patriots
- My Genie SE
- My GetRight
- NeatFTP
- 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
- NetSuck 3.10.5
- NetTime Thingy
- Network Assistant
- NeuroStock
- NewsBin
- NewsShark
- NewsWire
- NfoNak
- NotePads+
- Notificator 1.0b
- Octopus
- Pattern Book
- People Seek 98
- Personal Search Agent
- Photocopier
- PicPluck
- Pictures In News
- Ping Thingy
- PingMaster
- Planet.Billboard
- Planet.MP3Find
- PMS
- ProtectX 3
- ProxyChecker
- QuadSucker/Web
- Quadzle Puzzles
- QuikLink Autobot
- QuikLink Explorer
- QuikLink Explorer Gold Edition
- QuoteWatch
- QWallet
- Real Estate Web Site Creator
- Recipe Review
- ReGet 1.6
- Resume Detective
- RingSurf
- RoboCam 1.10
- Rosemary's Weird Web World
- SaberQuest Page Burner
- SBJV
- SBWcc
- Scout's Game
- ScreenFIRE
- ScreenFIRE - FileKing
- ScreenFlavors
- Sea Battle
- Shizzam
- Simple Submit
- SimpleFind
- SimpleSubmit v1.0
- SK-111
- Smart 'n Sticky
- SmartBoard 200 FREE Edition
- SmartSum calculator
- SonicMail
- Sound Agent
- Space Central Screen Saver
- Splash! Siterave
- StartDrive
- Static FTP
- StockNavegador
- Subscriber
- SunEdit 2K
- SuperIDE
- Sweep
- SweepsWinner
- Text Transmogrifier
- The Mapper
- TheNet
- TI-FindMail
- TIFNY
- Total Finger
- Total Whois
- Tracking The Eye
- Trade Site Creator
- TWinExplorer Standard
- TypeWriter 1.0
- UK Phone Codes
- 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
- VOG Shell History
- W3Filer
- Web Coupon
- Web Page Authoring Software
- Web Registrant PRO
- Web Resume
- Web SurfACE
- WEB2SMS
- WebCamVCR
- WebCopier
- Web-N-Force
- WebSaver
- Website Manager
- WebStripper
- WebType
- WhoIs Thingy
- Win A Lotto
- WinEdit 2000
- Word+
- Wordwright
- WorldChat Client
- Worm
- Devgames
- xBlock
- Your ESP Test
- Zion
- Zip Express 2000

5. Esta DLL envía la información siguiente a su servidor de todos las URL's que visitas:
   A.)Banners de los anuncios en que haces clic.
   B.)Todas las descargas que haces, muestra el nombre del fichero, tamaño, fecha, hora y tipo de archivo(imagen, zip, ejecutable...).
   C.)Las fechas y el tiempo de todas tus acciones mientras usas tu navegador.
   D.)El número de teléfono que marcas para conectar a Internet (sacado de la configuración del Acceso telefónico a redes).
   E.)La contraseña si esta guardada.
6. Contiene la nota de los programadores: "Show me the money! I want to be Mike!"

ADVPACK.DLL

Utilizado durante la instalación solamente controlar si hay otros ficheros necesarios.

AMCIS.DLL

Este DLL modifica los siguientes claves del registro:

1. HKEY_CURRENT_CONFIG
2. HKEY_DYN_DATA
3. HKEY_PERFORMANCE_DATA
4. HKEY_USERS
5. HKEY_LOCAL_MACHINE
6. HKEY_CURRENT_USER
7. HKEY_CLASSES_ROOT

Quita el registro de oleaut32.dll de la memoria suministrado por Microsoft y sustituye por sus propias llamadas. Lo registra de nuevo cuando el navegador se cierra. Crea los procesos que se comenzarán siempre que abras tu navegador.

AMCOMPAT.TLB

Este archivo sigue cualquier clip multimedia que uses.

Registra el tipo de archivo (video, imagen, sonido...), el título y su localización.

Contiene referencias a los DblClick.

AMSTREAM.DLL

Dispone comunicaciones en las dos direcciones tu sistema y el suyo.

Envía la información y recibe las actualizaciones commandos/archivos.

Abre el puerto 1749 para las comunicaciones.

SOLUCIONES

Uno puede pensar que conociendo los archivos espías, la forma de deshacerse de ellos seria borrarlos, es una solución, aunque no muy buena ya que el programa que los instalan suele dejar de funcionar si no están presentes.

Para librarse de estos molestos espías existen programas que buscan y eliminan archivos espías sin que por ello deje de funcionar el programa que los instalo.

Dos ejemplos de programas anti-espías podrían ser el OPOUT y el AD-WARE 4.5.

Estos y otros programas se pueden encontrar en las siguientes direcciones de Internet:

grc.com/optout.htm
www.lavasoft.de
www.zdnet-es.com.