Lecture content

1. **Spyware** (first 20 minutes)
   - What is it
   - Who produces it
   - How to get rid of it
2. **Examples of spyware** (20 minutes)
   - Kazaa
   - Gator
   - Realplayer
   - Aureate/Radiate
   - Hotbar
   - WebHancer

Spyware

- ***One Definition:***
  *Spyware is any software which employs a user's Internet connection in the background ("backchannel") **without their knowledge or explicit permission**. This gives the possibility of **information thefts**.*
  [*Steve Gibson, OptOut:* http://grc.com/optout.htm]

What spyware does

- Gather information
  - profile the user
  - statistical analysis of internet usage
- Active spyware
  - show adds
  - change banners
  - collect and deliver personal information to some third party
  - steal money (”stealware”)

About the terminology

- The meaning of the terms is a bit unclear
- Some define: spyware = adware
- Some define:
  - adware = legal software
  - spyware = illegal software
  - stealware = even more criminal
- This presentation:
  - Any technology that gathers information about a person or organization without their direct knowledge is considered spyware

Why spyware

- How small software companies get their money?
  - Traditional way are the license fees for users
  - Other way is to include adds in the software
    - what kind of adds?

Profiling and direct marketing

- For direct marketing
  - the user has to be profiled
  - google is doing the same thing
- Not illegal if
  - user is aware of profiling
  - privacy is guaranteed
  - questions where and who are not answered

Pros & cons

- Pros
  - Free or inexpensive software
- Cons
  - You have to trust that sensitive information is not analyzed
  - Slight performance drop
- Threats
  - “stealware”

How to get rid of spyware

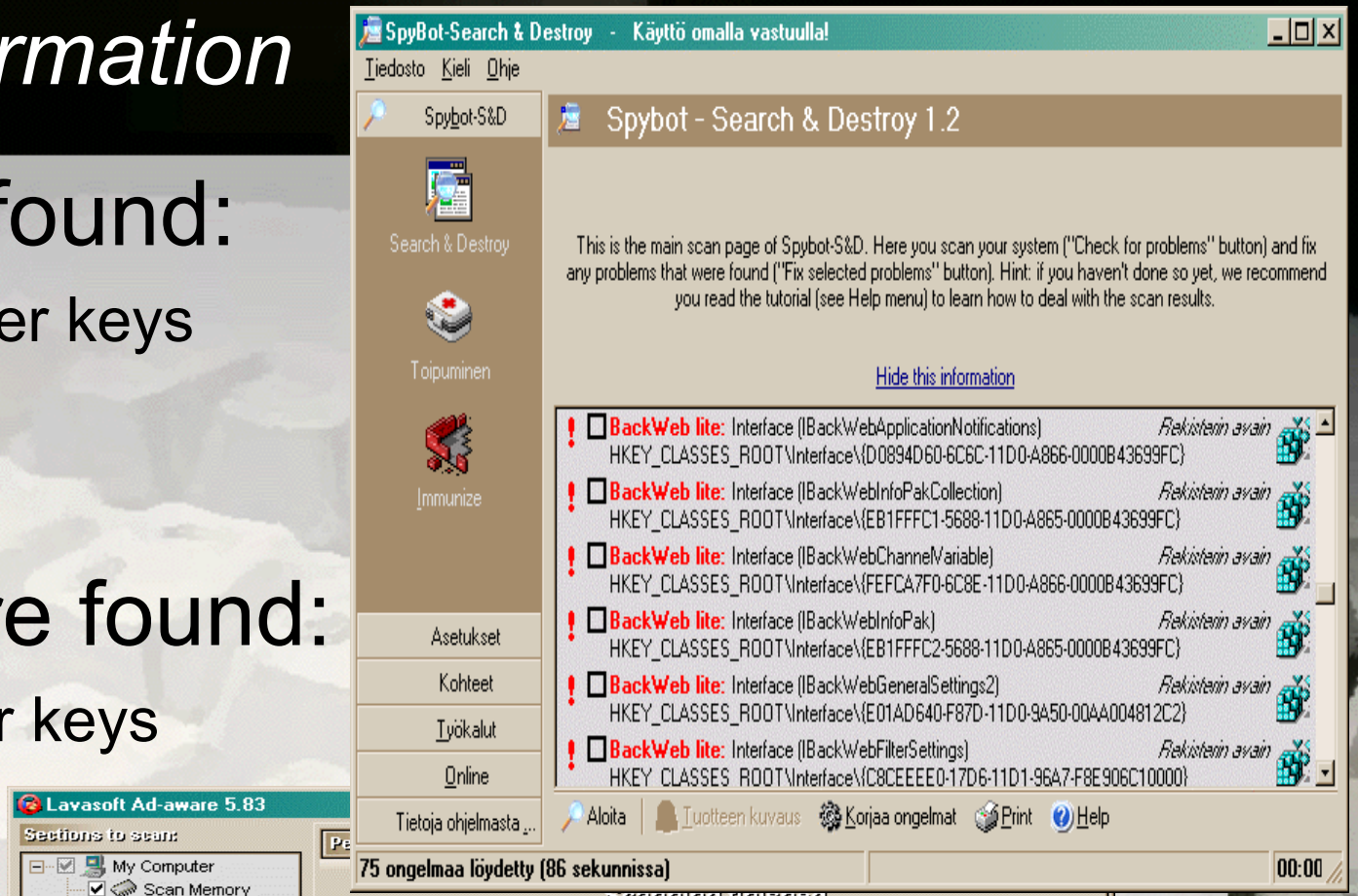
- Two basic methods
  - Make sure that the suspected programs can’t use the internet connection
  - Use a scanner to detect and remove all spyware
- Problems
  - You can’t always disable the internet connection from a program
  - Some scanners remove ‘too many’ binaries or register keys

Anti-spyware Software

- ZoneAlarm
  - Application layer firewall
  - www.zonelabs.com/
- Ad-aware
  - Spyware scanner (harddrive & windows registry)
  - http://www.lavasoftusa.com/

Practical information

- SpyBot found:
  - 67 register keys
  - 1 folder
  - 8 files
- Ad-aware found:
  - 5 register keys
  - 1 folder
  - 9 files



Links

- "OptOut" [http://grc.com/optout.htm]
  - Information, lists about known and suspected spyware
- "Threats of the information technology" [http://gamma.nic.fi/~tapio1/Opetus/Spyware.php3]
  - Information (both in FI and EN) and links
- Test how vulnerable your computer is
  - Tests [http://media.joensuu.fi/linkit/?l=Tietoturva]
- Spyware lists [http://www.tom-cat.com/spybase/index.html]

Examples of spyware

- Kazaa
- Gator
- Realplayer
- Aureate/Radiate
- Hotbar
- WebHancer

Kazaa

- **Popular file sharing software based on peer-to-peer technology**
- **Altnet – a subsidiary of Brilliant Digital Entertainment (BDE)**
- **Altnet's Secureinstall is bundled with BDE's b3d projector which is bundled with Kazaa**
- **b3d projector is installed for use of Altnet's network**
  - Any information about intended future use was not given prior to or during installation

Kazaa

- **Altnet uses peer-to-peer networking**
  - for its digital advertising technology
  - to distribute other companies' content
- **Altnet runs distributed computing**
  - Over their own network
  - Other peer-to-peer networks based on the same technology
- **Altnet can function without Kazaa running**

Gator

- **Helps you to fill out forms you frequently visit**
  - usernames
  - passwords
  - credit card information
- **Information is stored in an encrypted file**
  - Gator accesses this information using your IP address
- **Targets consumers based on site visitation and historical behaviour**
- **Provides aggregate statistics to third-party vendors about**
  - customers
  - traffic patterns
  - related site information

Gator

- **Dynamically inserts ads on top of existing ads on web pages**
  - Inserted ads look and feel like the site's real banners
  - Displays ads the web site never intended
    - e.g. ads for competitors' products
- **From their Privacy Policy:**
  "Please be aware that we sometimes use third party contractors who are given access to your profile to perform tasks that might otherwise be done by Gator.com employees.“

Gator

- Some version's of Gator's installer are blocked by Symantec's Norton AntiVirus (NAV)
- According to NAV, the Gator installer is infected with the Backdoor.Trojan
- Gator is available as a stand-alone application as well as bundled with other software

Realplayer

- **Full version possibly contains spyware agents**
- **Realplayer won't work anymore if those agents are removed**
- **Avoid their spyware agents from taking control by keeping RealPlayer from loading on startup**
- **It is recommended to use firewall when using Realplayer on the Net**
- **Disable any options from the Preferences that allow RP to call home**

Aureate/Radiate

- ”Granddaddy” of the spyware
- Can be instantly embedded in any software
  - gives advertisers the ability to target software users when they are using the software
- Is not stopped by firewalls
- Features
  - Can deliver
    - precise audience targeting
    - rich media
  - advertisements can be viewed offline

Aureate/Radiate

- More ”features”:
  - it deliberately slips into user’s system secretly
  - uses the user’s Internet backchannel without user’s permission or knowledge
  - instructs its hosting software to leave it installed upon host’s removal
  - masks its presence by deliberately suspending its use of the backchannel in the absence of keyboard or mouse activity

Hotbar

- **Free browser toolbar**
- **Collects and stores information (surprise!)**
  - URL of the web pages you view
  - data you enter in search engine search fields
  - your IP address
  - information about your browser
  - operating system
  - your Hotbar cookie number
  - data you enter in forms in web pages
  - toolbar buttons you click
  - the amount of time you have used it during each session
  - date/time the above information is logged
- **Serves ads from some well known networks**
- **5-star rating from ZDnet (common download center)**

WebHancer

- Provides a traffic measurement service that uses a client agent that is installed on user machines
- The Installation is hidden and triggered by the installation of software that is bundled with it
- Gathers information on
  - visited web page
    - address
    - page size
    - load time
    - completion state
  - Network delay time

WebHancer - Removal

- Incorrect removal procedures will destroy your Internet connection
- The Running WebHancer process appears in the Task List of Windows as Whagent
- Can be removed using Control Panel's Add/Remove Programs feature

WebHancer – Removal (2)

- Delete following files from Windows directory:
  webhdll.dll, whagent.inf, whInstaller.exe, whInstaller.ini
- Delete the WebHancer folder in your Program Files (if it still exists)
- Clean up your default Temp directory

Links

- List of known and suspected spyware
  [http://www.tom-cat.com/spybase/index.html]
- Information on most common spyware
  [http://www.simplythebest.net/info/spyware.html]
- ”Counterexploitation” web page
  [http://www.cexx.org/]