Peer to Peer Networks and Security

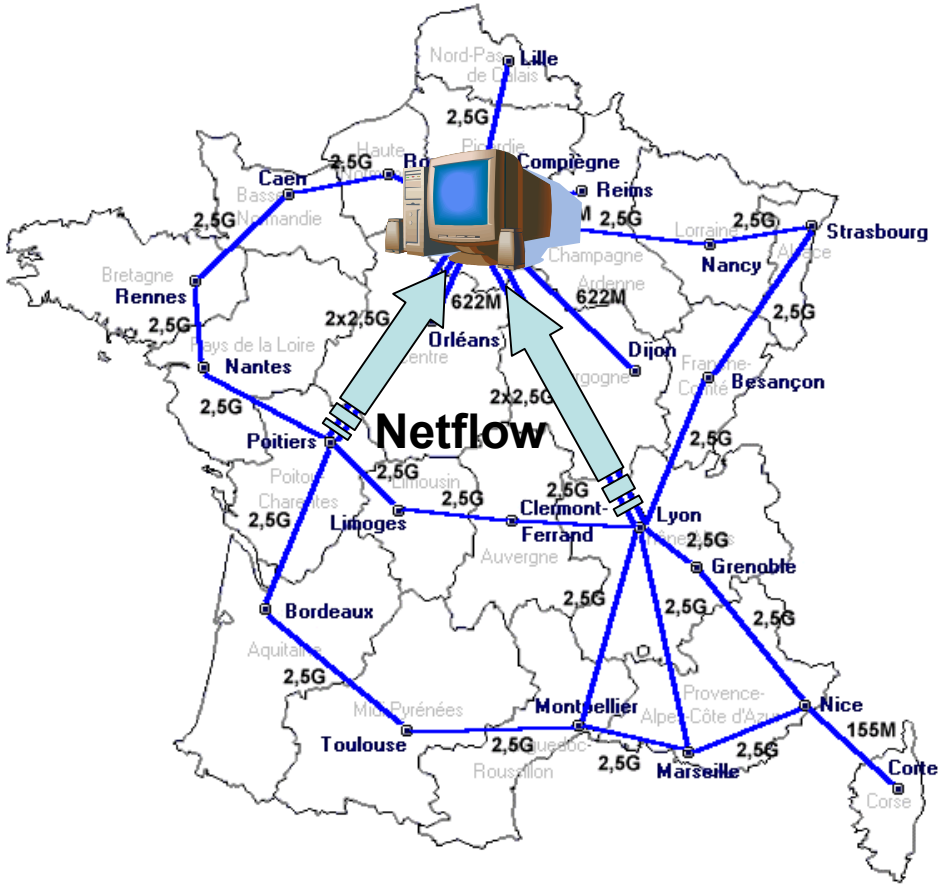
Kostya Kortchinsky
CERT RENATER
Kostya.Kortchinsky@renater.fr

Agenda

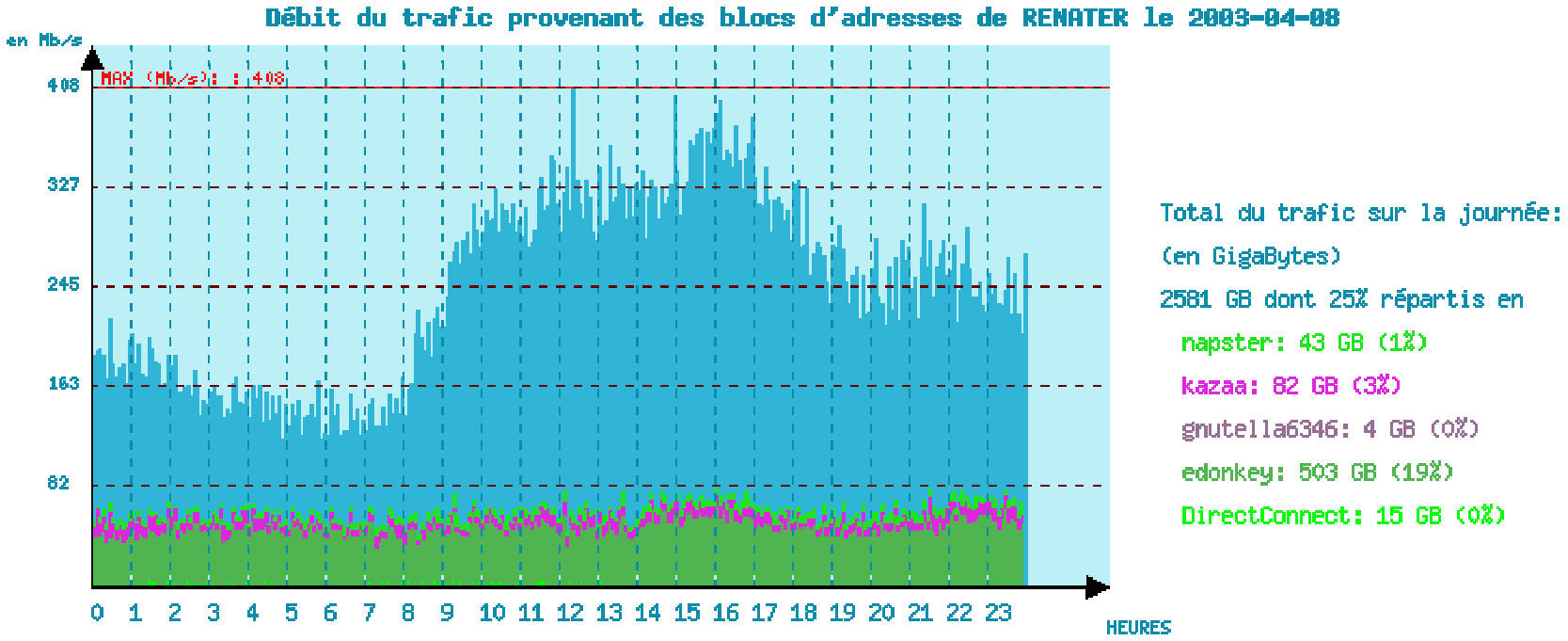
- Some Figures
- Security Issues
  - Viruses, trojans, and other malware
  - Information disclosure
  - System compromise
- Solutions

Some Figures

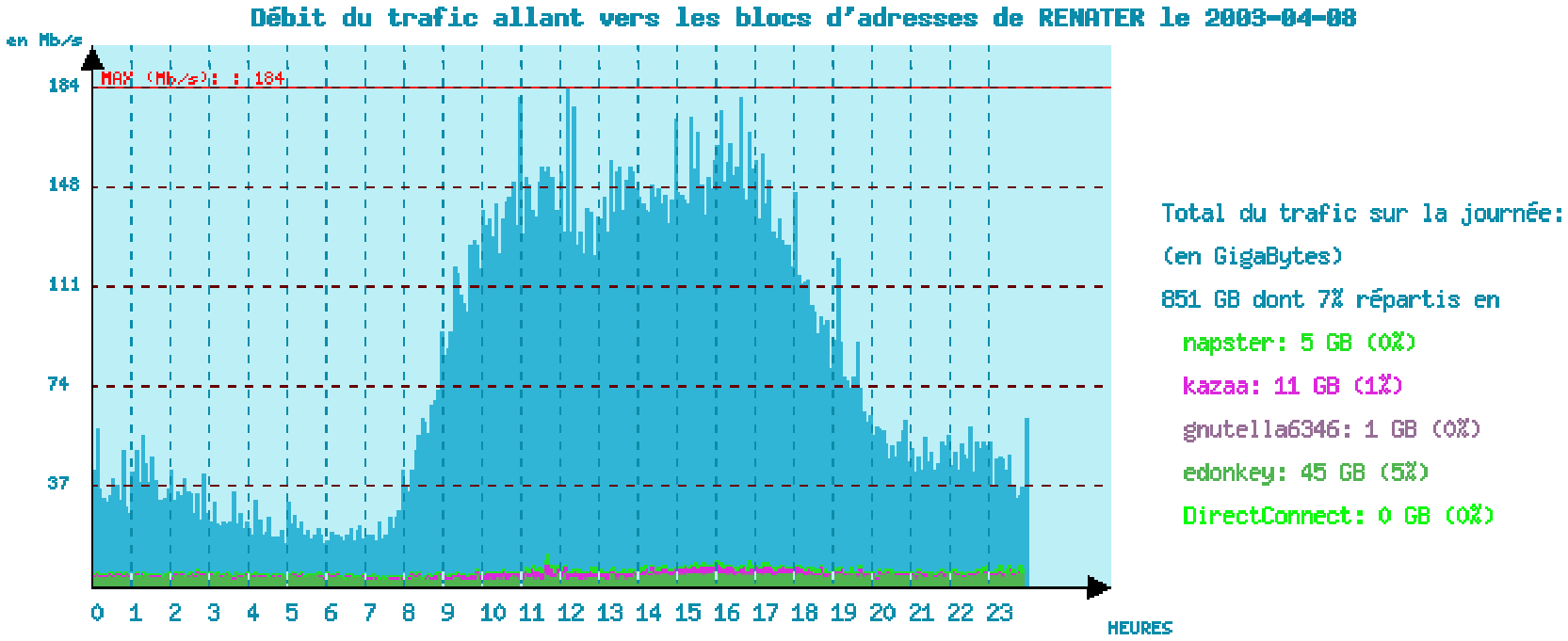
Traffic Monitoring on RENATER



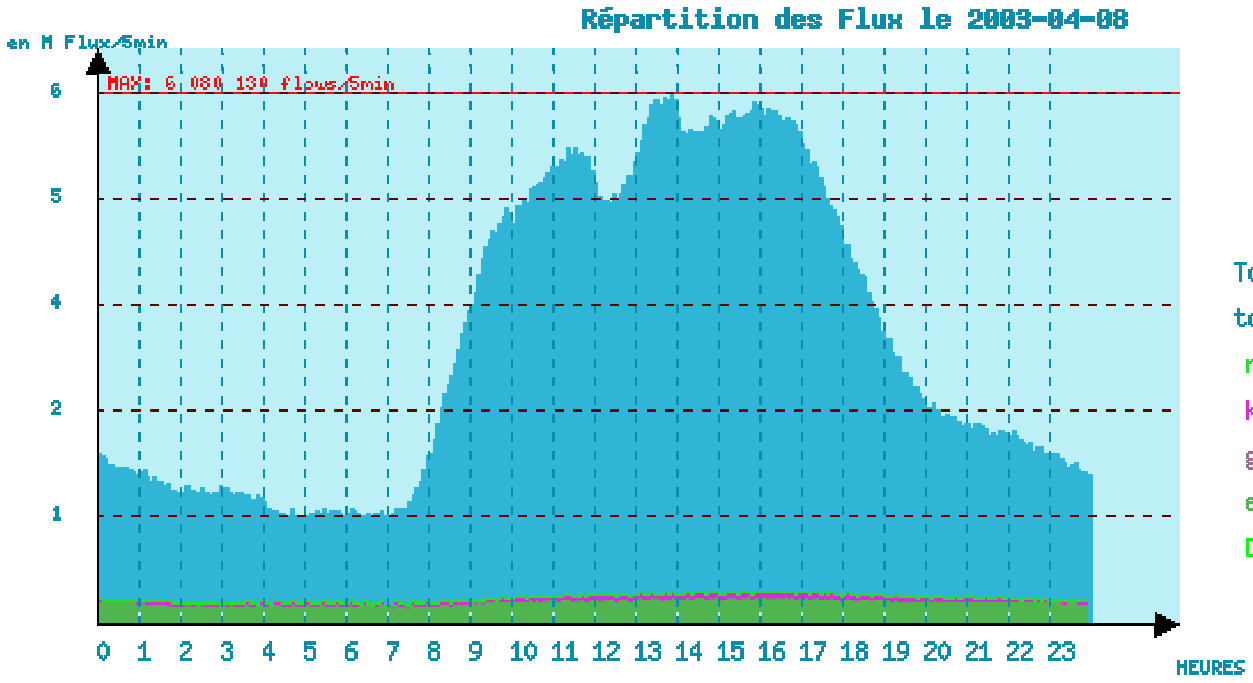
Traffic coming from RENATER



Traffic going to RENATER



Number of Flows



Total des Flows sur la journée:

total: 933 M dont 8% répartis en

napster: 0 M (0%)

kazaa: 7 M (0%)

gnutella6346: 1 M (0%)

edonkey: 74 M (7%)

DirectConnect: 0 M (0%)

Security Issues

Viruses, Trojans, and Other Malware

- A virus is a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event.
- A virus is often designed so that it is automatically spread to other computer users.
- Viruses can be transmitted as attachments to an e-mail note, as downloads, or be present on a diskette or CD.

Dissemination

THIS WEEK	Most Popular Titles in Windows Week Ending May 11	Last Week	Weeks On Chart	Downloads This Week	Total Downloads
1	**Kazaa Media Desktop** *popular* Search, download, and interact with a variety of files with this P2P file-transfer application. **OS:** Windows 95/98/NT/2000/XP **License:** Free	1	54	2,535,662	225,127,075
4	**iMesh** *popular* Find, download, and share MP3s and image files. **OS:** Windows (all) **License:** Free	4	159	427,542	49,234,312
7	**Morpheus** *popular new* Search for and exchange information with this P2P communication and file-sharing application. **OS:** Windows 95/98/NT/2000/XP **License:** Free	7	106	277,847	111,289,525

- By the software itself
  - Its popularity makes it a very valuable infection vector

DlDer

- http://www.grokster.com

  1 January 2002

  « It has recently come to our attention that our previous Grokster installer for about a three week period contained a program being called by the anti-virus companies W32.DlDer.Trojan. This program was apparently installed by one of our advertisers, ClickTilUWin. »

Dissemination

- By the content provided
  - Each user acts as a server for each other user
    - No centralized server to upload and download files
    - No way for the software developer to check the content provided
    - Protection is up to the user
  - A downloaded file is usually made available immediately for upload to other users

Dissemination

- http://www.kazaa.com/en/help/virus.htm

  « Most files that are accessible using Kazaa Media Desktop originate from other users. This means that there will always be the risk of irresponsible users introducing viruses. »

- P2P File-Sharing networks have become a very easy mean to spread viruses

Example

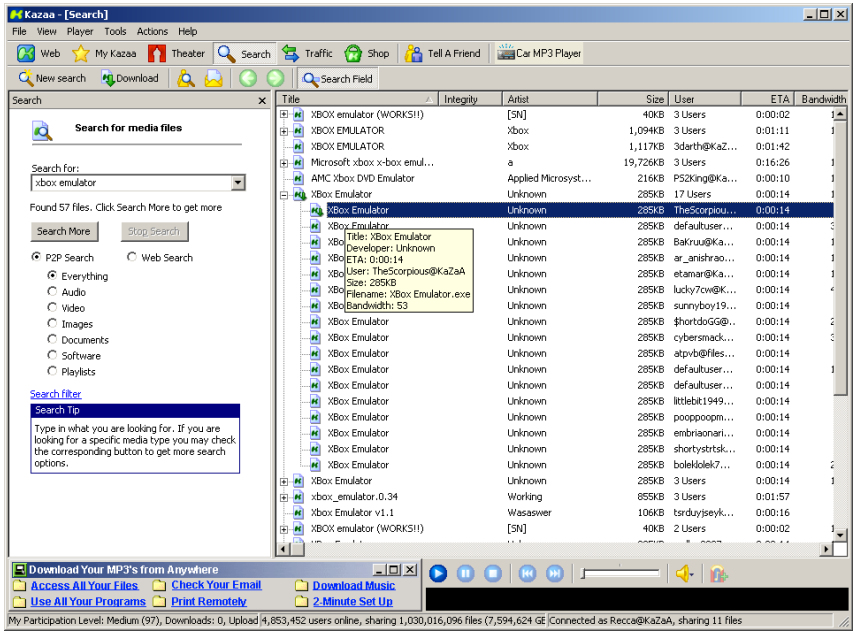
- Win32/Merkur.A@mm (2002-11-01)
  - Mass mailing Internet worm in VB6
  - Also spreads via
    - IRC network (using mIRC)
    - P2P network (using Kazaa, eDonkey, BearShare)
  - Copies itself to
    - C:\Program Files\Kazaa\My Shared Folder\IPspoofer.exe
    - C:\Program Files\Kazaa\My Shared Folder\Virtual Sex Simulator.exe

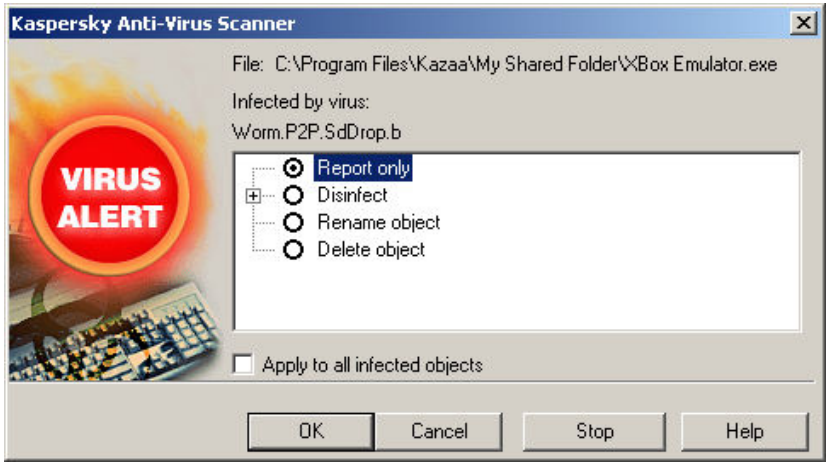
Example

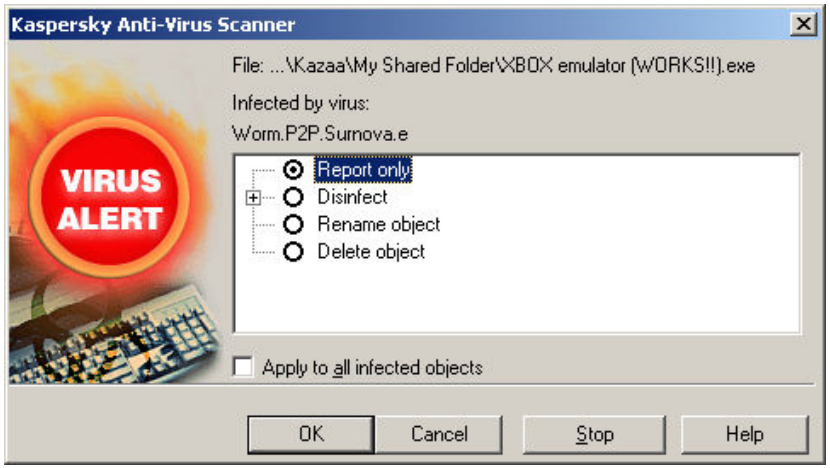
- Win32/HLLW.Gool.B (2003-02-14)
  - Backdoor with trojan and internet worm capabilities in Delphi
  - Sets in the registry the sharing folders for Kazaa to C:\Windows\Sys32
  - Copies itself in this folder to
    - Britney.jpg.exe
    - Catherine_Zeta_Jones_Nude.jpg.exe
    - X_Box_Emulator.txt.exe

Screenshot

XBOX Emulator search results on KaZaA

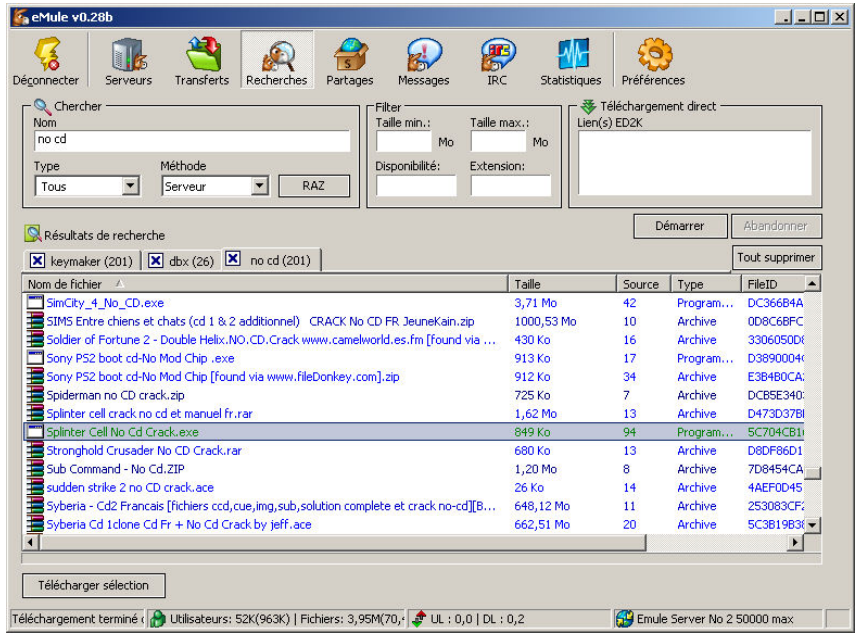


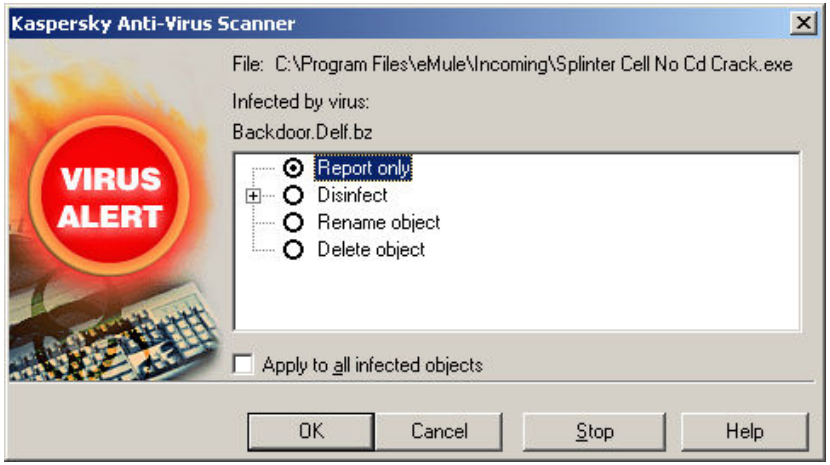


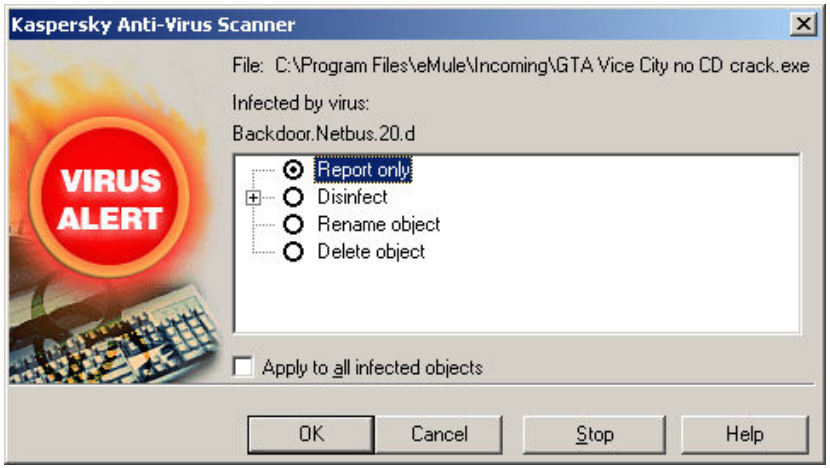


Screenshot

NO CD search results on eMule





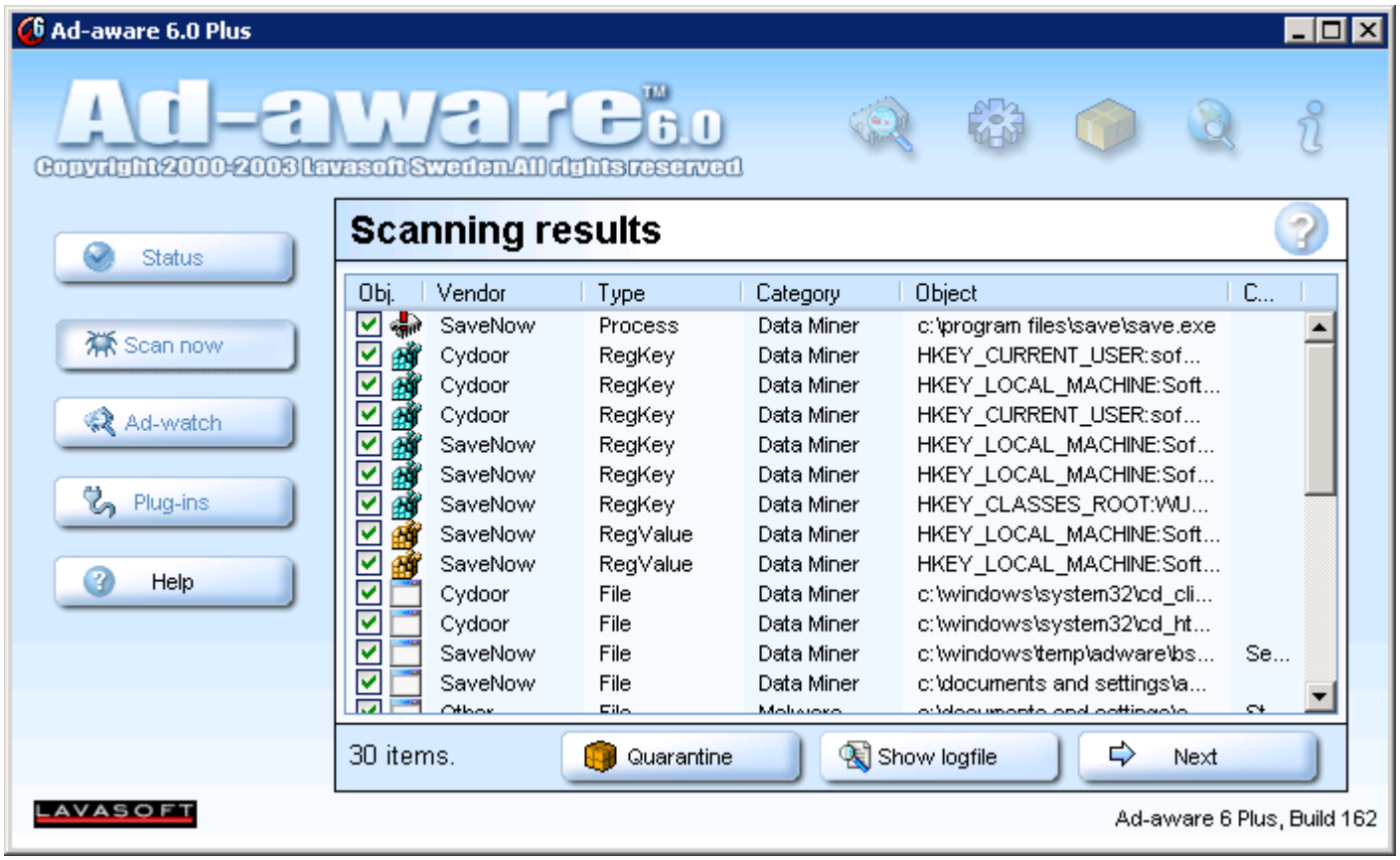


Information Disclosure

Spyware

- In general, spyware is any technology that aids in gathering information about a person or organization without their knowledge.
- On the Internet, spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties.

Screenshot

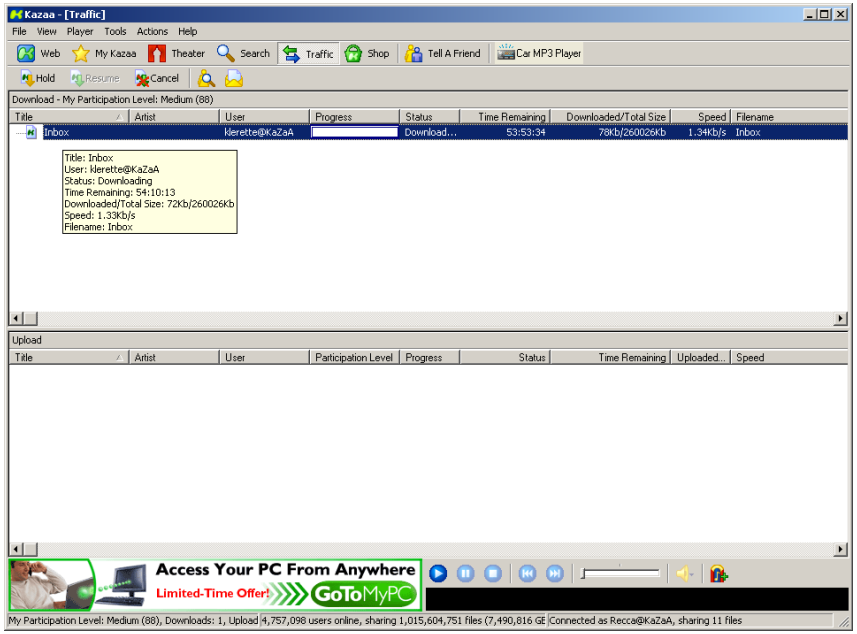

Ad-aware 6.0 Plus
Ad-aware 6.0
Copyright 2000-2003 Lavasoft Sweden. All rights reserved
Status
Scan now
Ad-watch
Plug-ins
Help
Scanning results
Obj. | Vendor | Type | Category | Object | C...
SaveNow | Process | Data Miner | c:\program files\save\save.exe
Cydoor | RegKey | Data Miner | HKEY_CURRENT_USER:sof...
Cydoor | RegKey | Data Miner | HKEY_LOCAL_MACHINE:Soft...
Cydoor | RegKey | Data Miner | HKEY_CURRENT_USER:sof...
SaveNow | RegKey | Data Miner | HKEY_LOCAL_MACHINE:Sof...
SaveNow | RegKey | Data Miner | HKEY_LOCAL_MACHINE:Sof...
SaveNow | RegKey | Data Miner | HKEY_CLASSES_ROOT:WU...
SaveNow | RegValue | Data Miner | HKEY_LOCAL_MACHINE:Soft...
SaveNow | RegValue | Data Miner | HKEY_LOCAL_MACHINE:Soft...
Cydoor | File | Data Miner | c:\windows\system32\cd_cli...
Cydoor | File | Data Miner | c:\windows\system32\cd_ht...
SaveNow | File | Data Miner | c:\windows\temp\adware\bs... | Se...
SaveNow | File | Data Miner | c:\documents and settings\a...
30 items.
Quarantine
Show logfile
Next
LAVASOFT
Ad-aware 6 Plus, Build 162

Sharing Private Data

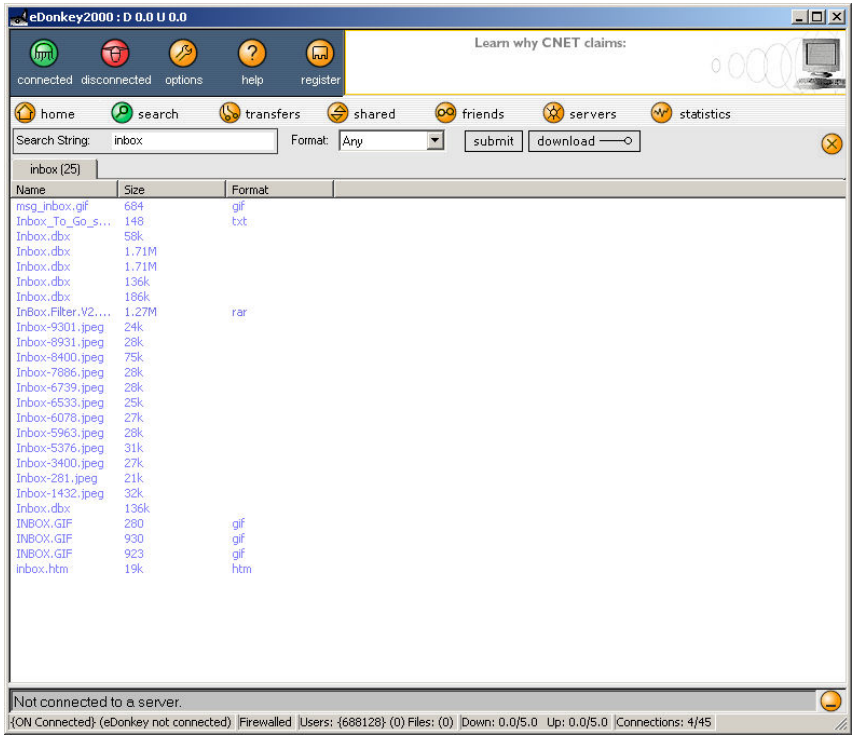
- The risk is great that unintended files will be shared
  - Users may often be sharing private data without being aware of it
  - Although theoretically the user controls what subdirectories he/she makes available to peer users, sometimes more subdirectories are shared than is known or intended

Screenshot

Downloading 260 megabytes **Inbox** file from KaZaA



Several **Inbox.dbx** in search results from eDonkey



Example

```
To: « Pierre Dupont » <pierre.dupont@xxxxxxx.fr>
Subject: Votre mot de passe
From: membre@yyyy.fr
Reply-To: membre@yyyy.fr
Date: Tue, 22 Oct 2002 18:29:37 +0200

Cher(e) membre,

Vous avez oublie votre mot de passe, le voici :
   zzzzzz

A tres bientot sur www.yyyy.fr
L'equipe Yyyy !
```

System Compromise

BearShare Advice

- http://www.bearshare.com/help/citizen.htm

  « You don't need to get rid of your firewall completely, you just need to "drill a hole" in it for BearShare. It won't decrease your security because BearShare doesn't contain any security holes. Please read BearShare Firewall Tutorial for instructions how to configure your firewall. »

BearShare Directory Traversal

- http://www.securityfocus.com/bid/5888

  « The BearShare webserver is prone to directory traversal attacks. This may allow remote attackers to break out of the web root directory and browse the filesystem of the host running the software.
  This issue is a variant of the vulnerability described in Bugtraq ID 2672. The variant issue was unsuccessfully addressed in version 4.0.6. It is still possible to disclose files with a malicious URL encoded request to the webserver. »

eDonkey 2000 Buffer Overflow

- http://www.securityfocus.com/bid/4951

  « The eDonkey 2000 Windows client includes a handler for a custom URI, ed2k://. It has been reported that the handler for eDonkey 2000 is vulnerable to a buffer overflow condition when parsing maliciously constructed URIs. This may be exploited to crash the user's browser or execute arbitrary code on the victim client. »

Kazaa Buffer Overflow

- http://www.securityfocus.com/bid/6747

  « KaZaA version 2.0.2 is vulnerable to a denial of service attack caused by a buffer overflow. By sending a malicious response to an affected system for the automated advertisement download, a remote attacker could overflow a buffer and cause the system to crash or possibly execute code on the system. »

SETI@home Buffer Overflow

- http://spoor12.edup.tudelft.nl

  « The SETI@home clients use the HTTP protocol to download new workunits, user information and to register new users. There is a bufferoverflow in the server responds handler. Sending an overly large string followed by a newline ('\n') character to the client will trigger this overflow. »

Solutions

JANET-CERT

- http://www.ja.net/CERT/JANET-CERT/prevention/peer-to-peer.html
  - « ...In an aim to improve the security of our network, as well as hopefully reduce bandwidth, particularly outgoing, we have decided to block Peer To Peer (P2P) file sharing. Research has revealed the following TCP/IP are used, and the software that uses them. Links to the software itself can be found with the list of ports... »

University of Chicago

- Disabling Peer to Peer File Sharing
  - http://security.uchicago.edu/peer-to-peer/no_fileshare.shtml

Thank You !
Questions ?