Peer to Peer Networks and Security

Kostya Kortchinsky CERT RENATER Kostya.Kortchinsky@renater.fr

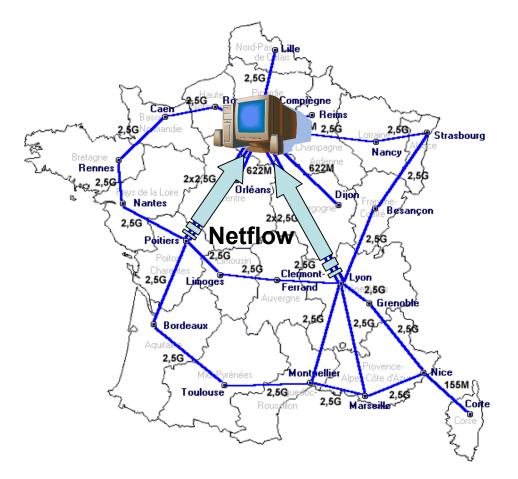
Agenda

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

Some Figures

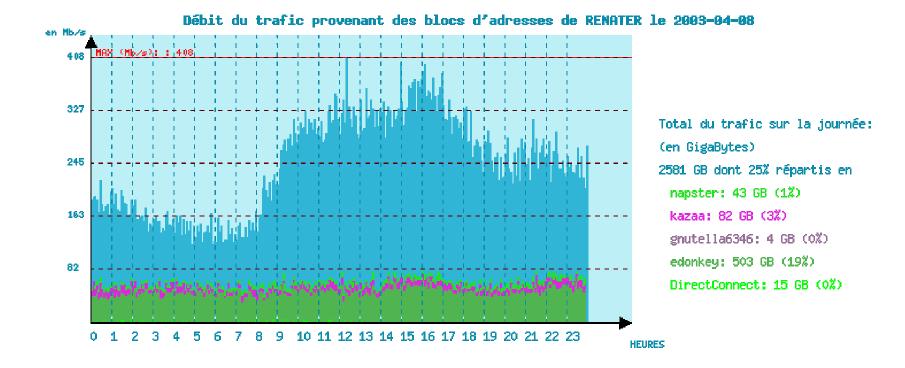
23/06/2003

Traffic Monitoring on RENATER

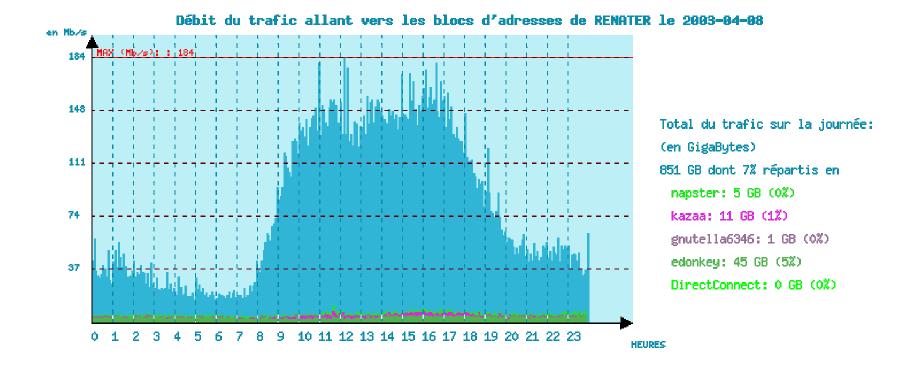


Kostya Kortchinsky - RENATER

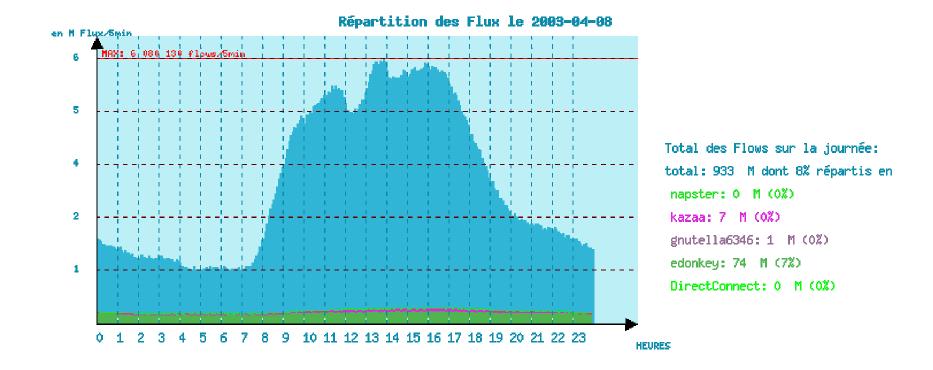
Traffic coming from RENATER



Traffic going to RENATER



Number of Flows



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	<u>Kazaa Media Desktop</u> <i>popular</i> 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 <i>popular</i> 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

DIDer

<u>http://www.grokster.com</u>

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.DIDer.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

<u>http://www.kazaa.com/en/help/virus.htm</u>

 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

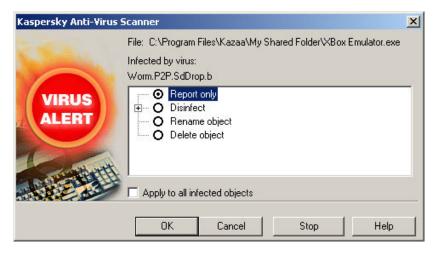
Example

- 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

Kazaa - [Search]						
ile View Player Tools Actions Help						
🔀 Web 👷 My Kazaa 👖 Theater 🔍 Sean	h 🔄 Traffic 💮 Shop 😤 Tell A Friend	Car MP3 Player				
🔾 New search M Download 🛕 🍋 🙆	Search Field					
iearch >	Title △ Integrity Title △ Integrity	Artist [SN]	Size User 40KB 3 Users	ETA Band 0:00:02		
Search for media files	THE A XBOX EMULATOR	Xbox	1.094KB 3 Users	0:01:11		
<u> </u>	XBOX EMULATOR	Xhox	1.117KB 3darth@KaZ	0:01:42		
	Microsoft xbox x-box emul	a	19.726KB 3 Users	0:16:26		
Search for:	AMC Xbox DVD Emulator	Applied Microsyst	216KB P52King@Ka	0:00:10		
xbox emulator	- A XBox Emulator	Unknown	285KB 17 Users	0:00:14		
Found 57 files. Click Search More to get more	XBox Emulator	Unknown	285KB TheScorpiou	0:00:14		
	XBox Emulator	Unknown	285KB defaultuser	0:00:14		
Search More Stop Search	XBo Title: XBox Emulator	Unknown	285KB BaKruu@Ka	0:00:14		
P2P Search O Web Search	XB0 ETA: 0:00:14	Unknown	285KB ar anishrao	0:00:14		
Everything	XBo User: TheScorpious@KaZaA	Unknown	285KB etamar@Ka	0:00:14		
C Audio	XBo Filename: XBox Emulator.exe	Unknown	285KB lucky7cw@K	0:00:14		
O Video	XBo Bandwidth: 53	Unknown	285KB sunnyboy19	0:00:14		
C Images	XBox Emulator	Unknown	285KB \$hortdoGG@	0:00:14		
O Documents	XBox Emulator	Unknown	285KB cybersmack	0:00:14		
O Software	XBox Emulator	Unknown	285KB atpvb@files	0:00:14		
C Playlists	XBox Emulator	Unknown	285KB defaultuser	0:00:14		
	XBox Emulator	Unknown	285KB defaultuser	0:00:14		
Search filter	XBox Emulator	Unknown	285KB littlebit1949	0:00:14		
Search Tip	XBox Emulator	Unknown	285KB pooppoopm	0:00:14		
Type in what you are looking for. If you are looking for a specific media type you may check	XBox Emulator	Unknown	285KB embriaonari	0:00:14		
the corresponding button to get more search	XBox Emulator	Unknown	285KB shortystrtsk	0:00:14		
options.	XBox Emulator	Unknown	285KB boleklolek7	0:00:14		
	💿 🛃 XBox Emulator	Unknown	285KB 3 Users	0:00:14		
	😟 🛃 xbox_emulator.0.34	Working	855KB 3 Users	0:01:57		
		Wasaswer	106KB tsrduyjseyk	0:00:16		
	E M XBOX emulator (WORKS!!)	[5N]	40KB 2 Users	0:00:02		
			000UD 8 0000	· ·		
Download Your MP3's from Anywhere				-		
Access All Your Files Check Your Email] 🛛 🖸 📘				
Use All Your Programs C Print Remotely	2-Minute Set Up					
Participation Level: Medium (97), Downloads: 0, Upload		T FOA COA OF COMPANY	- Descentive Test schedules 44 films			
Participation Level: Medium (97), Downloads: U, Upload	,000,402 users online, snanng 1,000,016,096 hles (7,594,624 GE Juonnected a	s Recca@RazaA, sharing 11 hies			



Kaspersky Anti-Virus	Scanner	×
	File:\Kazaa\My Shared Folder\XB0X emulator (W0RKS!!).exe Infected by virus: Worm.P2P.Surnova.e	
VIRUS	 Report only Disinfect Rename object Delete object 	
A CE	Apply to all infected objects	
	OK Cancel <u>S</u> top Help	

Kostya Kortchinsky - RENATER

Screenshot

NO CD search results on eMule

Image: Serveurs Image: Serveurs <th< th=""><th>nax.: Mo</th><th>Préféren léchargem ED2K</th><th></th><th></th></th<>	nax.: Mo	Préféren léchargem ED2K		
Résultats de recherche		Dé	imarrer	Abandonner
keymaker (201) X dbx (26) X no cd (201)			[Tout supprimer
om de fichier	Taille	Source	Туре	FileID -
SimCity_4_No_CD.exe	3,71 Mo	42	Program	DC366B4A
SIMS Entre chiens et chats (cd 1 & 2 additionnel) CRACK No CD FR JeuneKain.zip	1000,53 Mo	10	Archive	0D8C6BFC
Soldier of Fortune 2 - Double Helix.NO.CD.Crack www.camelworld.es.fm [found via	430 Ko	16	Archive	3306050DE
Sony PS2 boot cd-No Mod Chip .exe	913 Ko	17	Program	D3890004(
Sony PS2 boot cd-No Mod Chip [found via www.fileDonkey.com].zip	912 Ko	34	Archive	E3B4B0CA:
Spiderman no CD crack.zip	725 Ko	7	Archive	DCB5E340:
Splinter cell crack no cd et manuel fr.rar	1,62 Mo	13	Archive	D473D37BI
Splinter Cell No Cd Crack.exe	849 Ko	94	Program	5C704CB1
Stronghold Crusader No CD Crack.rar	680 Ko	13	Archive	D8DF86D1
Sub Command - No Cd.ZIP	1,20 Mo	8	Archive	7D8454CA
sudden strike 2 no CD crack.ace	26 Ko	14	Archive	4AEF0D45
	648,12 Mo	11	Archive	253083CF2
Syberia - Cd2 Francais [fichiers ccd,cue,img,sub,solution complete et crack no-cd][B	662,51 Mo	20	Archive	5C3B19B3(-
Syberia - Cd2 Francais [richiers ccd,cue,img,sub,solution complete et crack no-cd][B Syberia Cd 1clone Cd Fr + No Cd Crack by jeff.ace	662,51 MO			





Kostya Kortchinsky - RENATER

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

6 Ad-aware 6.0 Plus							
			1		เ		
Status	Scanning results						
	Obj. Vendor	Туре	Category	Object	C		
Can now Category Cate	Image: SaveNow Image:	Process RegKey RegKey RegKey RegKey RegKey RegKey RegValue RegValue File	Data Miner Data Miner Data Miner Data Miner Data Miner Data Miner Data Miner Data Miner Data Miner	c:\program files\save\save.exe HKEY_CURRENT_USER:sof HKEY_LOCAL_MACHINE:Soft HKEY_CURRENT_USER:sof HKEY_LOCAL_MACHINE:Sof HKEY_LOCAL_MACHINE:Sof HKEY_LOCAL_MACHINE:Soft HKEY_LOCAL_MACHINE:Soft HKEY_LOCAL_MACHINE:Soft c:\windows\system32\cd_cli			
LAVASOFT	Cydoor SaveNow SaveNow SaveNow Other 30 items.	File File File File Cuarantine	Data Miner Data Miner Data Miner Melecere	c:\windows\system32\cd_ht c:\windows\temp\adware\bs c:\documents and settings\a c:\documents ond settings\a how logfile	Se		

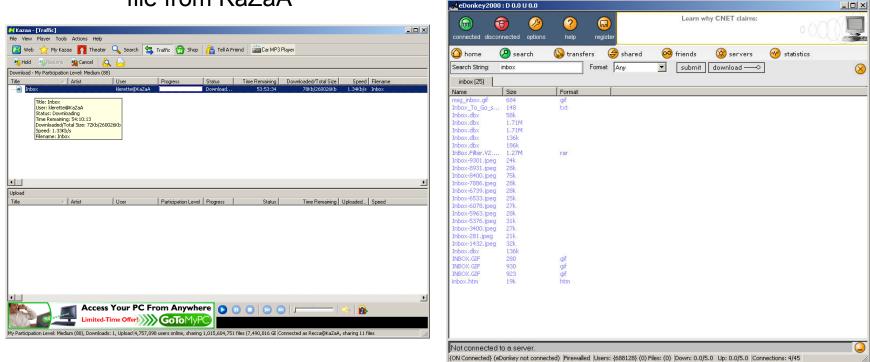
Sharing Private Data

- 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@xxxxxx.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 : zzzzz

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

System Compromise

BearShare Advice

- <u>http://www.bearshare.com/help/citizen.htm</u>
 - « 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

- <u>http://www.securityfocus.com/bid/5888</u>
 - « 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

- <u>http://www.securityfocus.com/bid/4951</u>
 - « 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

- <u>http://www.securityfocus.com/bid/6747</u>
 - « 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

- <u>http://spoor12.edup.tudelft.nl</u>
 - « 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

- <u>http://www.ja.net/CERT/JANET-</u> <u>CERT/prevention/peer-to-peer.html</u>
 - « ...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
 - <u>http://security.uchicago.edu/peer-to-peer/no_fileshare.shtml</u>

Thank You ! Questions ?