How to remove rontok baca bro second limited lazy edition

By Faisal / Myvwa + Myvwaca
Greets: F A / Myvwa + Myvwaca

It’s 12:24 am when I wrote this article.. I had a flu damn:winston, malboro, harvest, dunhill .. they make me sick..now I wanna sleep but I can’t.. I wanna study but I can’t .. my brain don’t work well also my lung, unstable heart’s beat too..

+==================+
+Minimum Requirement+
+==================+

Heh! Of course this article need some requirements..
The requirement for the people to reading this article is

1. Must have an Ability to read the broken english article.(plz convert English to malay ;p)
2. Computer or any sort of viewer to view this article
3. Being able to understand the word that I type ;p
4. Fresh mind.. please don’t read it when you pre-sleep, sleep or sleep talking ;p
5. your friends Windows XP sp2 that are already infected with rontokbro.
6. You must can make sure that you know **WINDOWS XP SP2** Characteristics.. not the vendor machine ;p

ok I won’t take responsibilities about the damage that may be occur while practicing the true of lazy manual of mine.. sorry I’m so lazy.. but this is the way I kill my time..

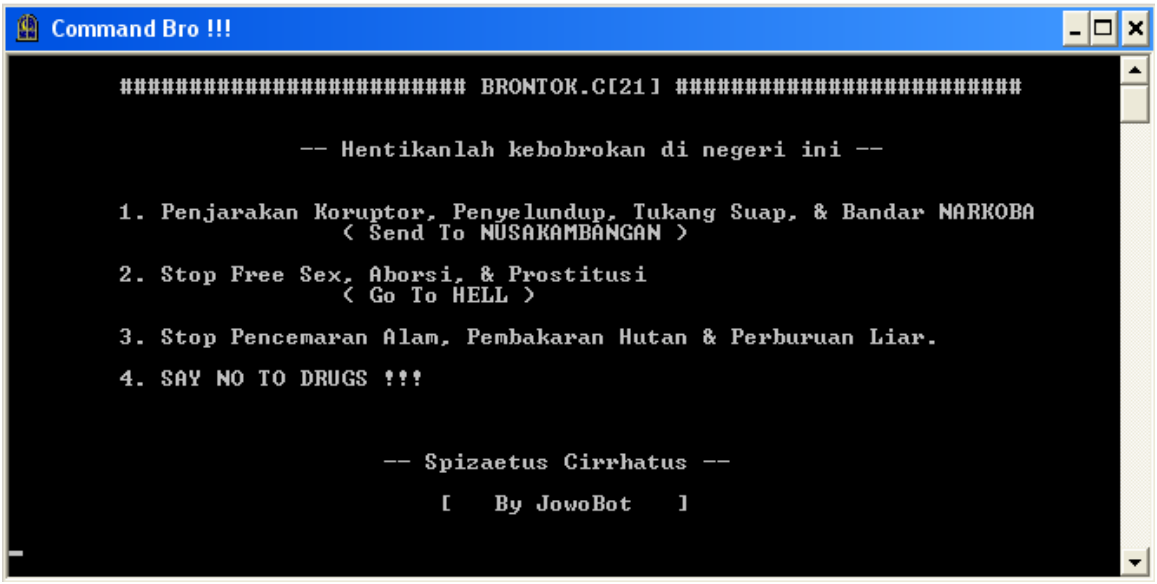
I need to install the brontok.. damn brontok where are you.. ahaaaa.. yeah..

Ok.. after you reboot.. please don’t open any folder. Don’t open your my Computer too.. please..

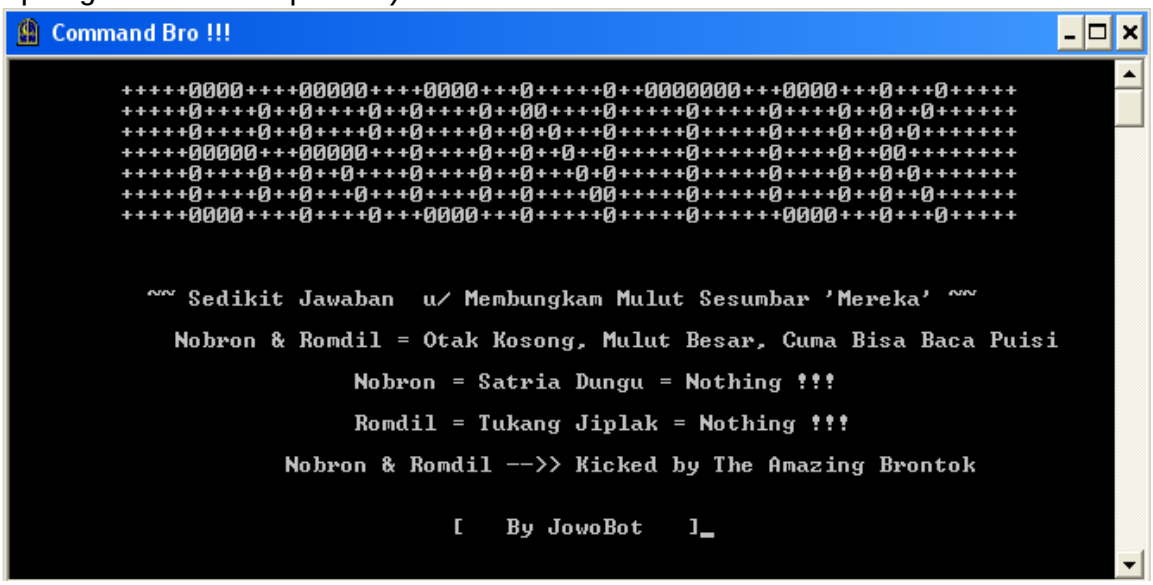
```
#include <windows.h>
#include <small.h>
int main()
{
     while(1)
     {
          MessageBox(NULL,”Why? When? What?”,”?”,MB_OK);
     }
return 0;
}
/********small.h********
#pragma comment(linker,"/ENTRY:main")
#pragma comment(linker,"/MERGE:.rdata=.data")
#pragma comment(linker,"/MERGE:.text=.data")
#pragma comment(lib,"msvcrt.lib")
#if (_MSC_VER < 1300)
     #pragma comment(linker,"/IGNORE:4078")
     #pragma comment(linker,"/OPT:NOWIN98")
#endif

#define WIN32_LEAN_AND_MEAN
EOF **********/
```

Sorry.. the above code is for release tension purposed..
don’t compile and run.. heh.. I hope you test it..

Ok.. let go to start->run->notepad C:\Baca Bro !!!.txt
You will get this politic motivation message..

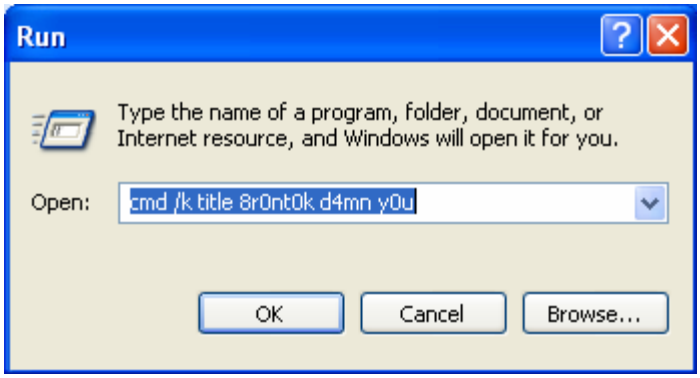


And the other message.. I think the author of this worm wanna express himself that NoBron and Romdil can't stop him… I don't know who is mulut besar(I think "cakap besar") And Romdil who is a tukang jiplak(I think he wanna say "plagiat aka ciplak")

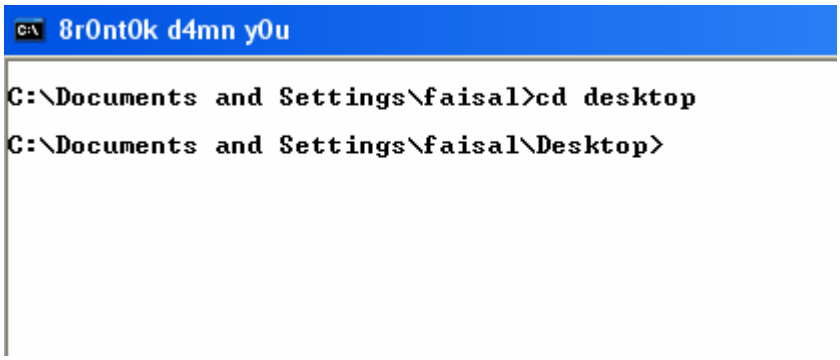


Yeah Brontok.C[21].. nice armor dude.. nice message too..

Ok.. start->run
Type this command "cmd /k title 8r0nt0k d4mn y0u" without quote..



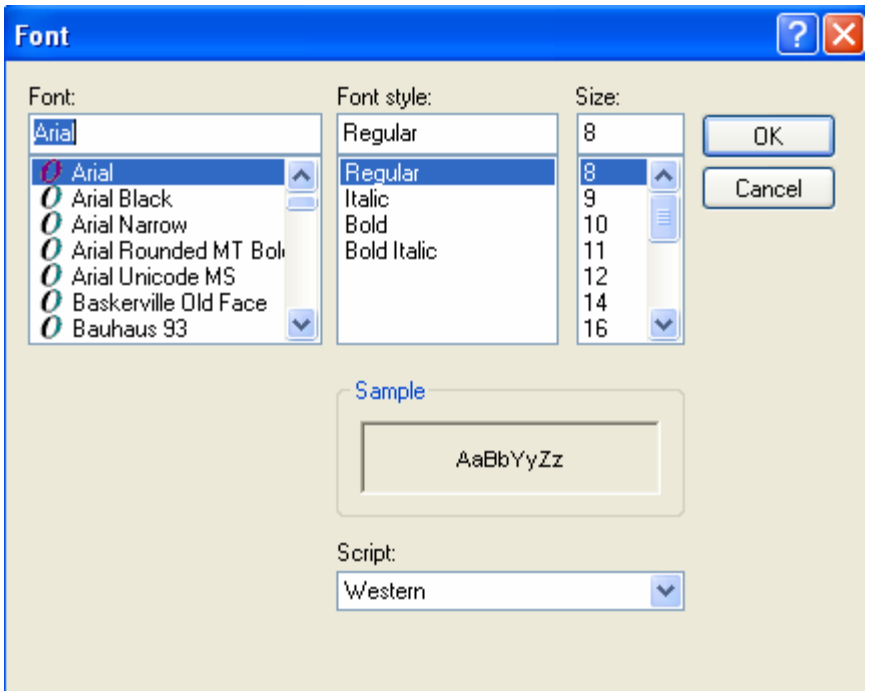
Then type “cd desktop” at the command prompt



Ok.. same tools..
cmd.exe,tasklist.exe and tskill.exe

ok please type “tasklist /v>asmah.txt”

Open asmah.txt then change he format of font by click at format->font



Use the arial with the size of 8.. and you can read without stress feeling

Please open the asmah.txt.. then you got this info

Image Name	PID	Session Name	Session#	Mem Usage	Status	User Name	CPU Time	Window Title
System Idle Process	0	Console	0	16 K	Running	NT AUTHORITY\SYSTEM	10:12:56	N/A
System	4	Console	0	240 K	Running	NT AUTHORITY\SYSTEM	0:00:34	N/A
smss.exe	712	Console	0	372 K	Running	NT AUTHORITY\SYSTEM	0:00:00	N/A
csrss.exe	784	Console	0	1,868 K	Running	NT AUTHORITY\SYSTEM	0:00:12	N/A
winlogon.exe	808	Console	0	2,708 K	Running	NT AUTHORITY\SYSTEM	0:00:01	N/A
services.exe	852	Console	0	4,008 K	Running	NT AUTHORITY\SYSTEM	0:00:03	N/A
lsass.exe	864	Console	0	1,312 K	Running	NT AUTHORITY\SYSTEM	0:00:01	N/A
svchost.exe	1020	Console	0	4,680 K	Running	NT AUTHORITY\SYSTEM	0:00:00	N/A
svchost.exe	1076	Console	0	4,144 K	Running	NT AUTHORITY\NETWORK SERVICE	0:00:00	N/A
svchost.exe	1416	Console	0	16,224 K	Running	NT AUTHORITY\SYSTEM	0:00:02	N/A
svchost.exe	1484	Console	0	2,776 K	Running	NT AUTHORITY\NETWORK SERVICE	0:00:00	N/A
svchost.exe	1552	Console	0	4,264 K	Running	NT AUTHORITY\LOCAL SERVICE	0:00:00	N/A
spoolsv.exe	1944	Console	0	6,404 K	Running	NT AUTHORITY\SYSTEM	0:00:10	N/A
explorer.exe	160	Console	0	28,000 K	Running	FAISAL-F777E41F\faisal	0:03:52	N/A
jusched.exe	260	Console	0	1,912 K	Running	FAISAL-F777E41F\faisal	0:00:00	OleMainThreadWndName
rundll32.exe	300	Console	0	2,700 K	Running	FAISAL-F777E41F\faisal	0:00:00	MediaCenter
acrotray.exe	384	Console	0	2,128 K	Running	FAISAL-F777E41F\faisal	0:00:00	AcrobatTrayIcon
inetinfo.exe	1744	Console	0	7,508 K	Running	NT AUTHORITY\SYSTEM	0:00:00	N/A
MDM.EXE	900	Console	0	2,652 K	Running	NT AUTHORITY\SYSTEM	0:00:00	N/A
sqlservr.exe	1840	Console	0	6,192 K	Running	NT AUTHORITY\NETWORK SERVICE	0:00:05	N/A
nvsvc32.exe	1872	Console	0	2,868 K	Running	NT AUTHORITY\SYSTEM	0:00:00	NVSVCPMMWindowClass
tomcat5.exe	488	Console	0	24,128 K	Running	NT AUTHORITY\SYSTEM	0:00:31	N/A
vmware-authd.exe	576	Console	0	3,420 K	Running	NT AUTHORITY\SYSTEM	0:00:54	N/A
vmnat.exe	352	Console	0	1,852 K	Running	NT AUTHORITY\SYSTEM	0:00:00	N/A
vmnetdhcp.exe	1688	Console	0	1,584 K	Running	NT AUTHORITY\SYSTEM	0:00:00	N/A
winamp.exe	3176	Console	0	14,412 K	Running	FAISAL-F777E41F\faisal	0:00:13	1. Raihan - Assubhubada - Winamp
WINWORD.EXE	548	Console	0	32,804 K	Running	FAISAL-F777E41F\faisal	0:00:51	test.doc - Microsoft Word
WISPTIS.EXE	3424	Console	0	5,420 K	Running	FAISAL-F777E41F\faisal	0:00:00	N/A
winlogon.exe	**1120**	**Console**	**0**	**4,048 K**	**Running**	**FAISAL-F777E41F\faisal**	**0:00:01**	**~Brontok~Is~The~Best~**
services.exe	**976**	**Console**	**0**	**3,100 K**	**Running**	**FAISAL-F777E41F\faisal**	**0:00:11**	**~Brontok~Serv~**
csrss.exe	**528**	**Console**	**0**	**2,636 K**	**Running**	**FAISAL-F777E41F\faisal**	**0:00:03**	**~Brontok~SpreadMail~**
lsass.exe	**1028**	**Console**	**0**	**4,420 K**	**Running**	**FAISAL-F777E41F\faisal**	**0:00:01**	**~Brontok~Network~**
ib7296.exe	**600**	**Console**	**0**	**3,832 K**	**Running**	**FAISAL-F777E41F\faisal**	**0:00:06**	**~Brontok~Back~Log~**
b7296.exe	**480**	**Console**	**0**	**3,820 K**	**Running**	**FAISAL-F777E41F\faisal**	**0:00:06**	**~Brontok~Back~Log~**
mspaint.exe	3876	Console	0	18,796 K	Running	FAISAL-F777E41F\faisal	0:00:04	untitled - Paint
svchost.exe	3864	Console	0	4,064 K	Running	NT AUTHORITY\SYSTEM	0:00:00	N/A
mspaint.exe	1124	Console	0	13,296 K	Running	FAISAL-F777E41F\faisal	0:00:01	untitled - Paint
cmd.exe	1936	Console	0	2,448 K	Running	FAISAL-F777E41F\faisal	0:00:00	8rOntOk d4mn yOu - tasklist /v
tasklist.exe	4028	Console	0	4,392 K	Running	FAISAL-F777E41F\faisal	0:00:00	OleMainThreadWndName
wmiprvse.exe	3584	Console	0	5,444 K	Running	NT AUTHORITY\NETWORK SERVICE	0:00:00	N/A

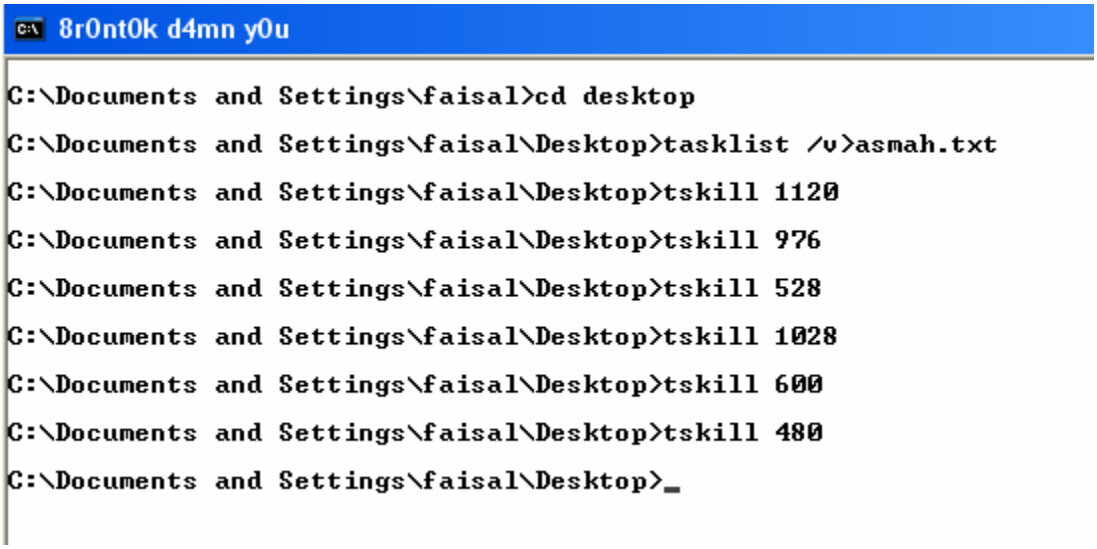
ok I coloured the brontok process to red color.. if you can't see them then I think you are the colour blinded person.. please ask your friends nicely to help you.. if they don't wanna help.. I think they have the same disease.. if it happened.. then ask your friends which not wear any extra eye and don't have any traffic violation.. get help from them..

ok please look at the **PID** which have the same row as brontok **Window Title**

my brontok's PID is **1120,976,528,1028,600,480**

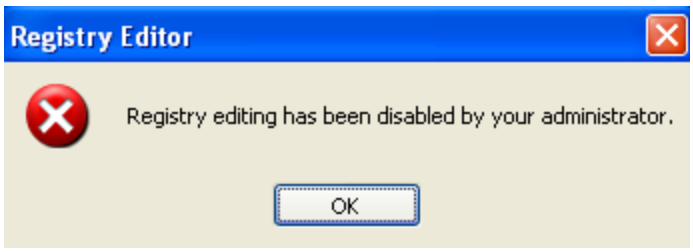
now we going to terminate them.. search and destroy baby..

please type at your command prompt
“tskill brontok’s PID”



Now all dead..
Ok

We need to clean the registry before we open any folder



Damn.. the brontok already disable it..
Ok.. never mind..

Open the notepad and type this

==========8< cut here==========

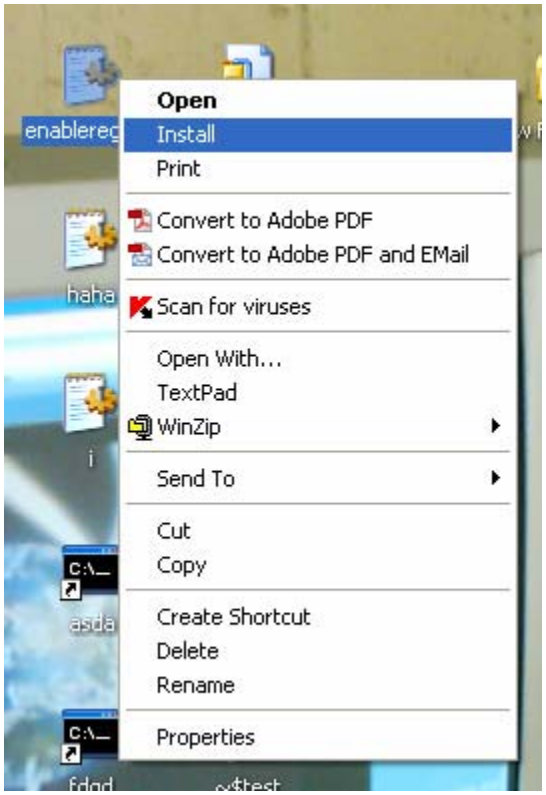
```
[version]
signature=$chicago$
[defaultinstall]
delreg=killbro
[killbro]
HKCU,Software\Microsoft\Windows\CurrentVersion\Policies\System,"DisableRegistryTools"
HKLM,Software\Microsoft\Windows\CurrentVersion\Policies\System,"DisableRegistryTools"
[End]
```

==========8< cut here==========

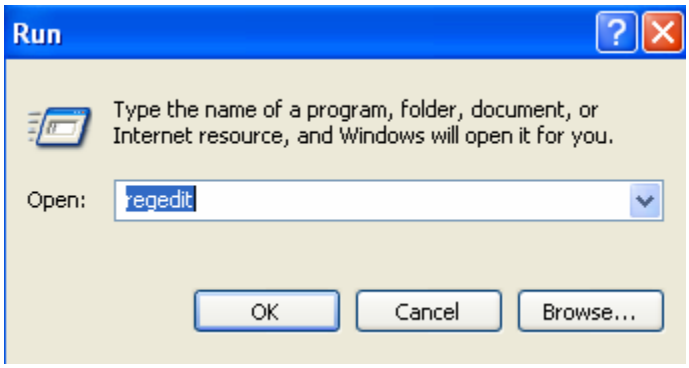
Then save as
Change the type to All Files and click at save

After that please look at your desktop fine the file enableregedit

Right click at that file and click install

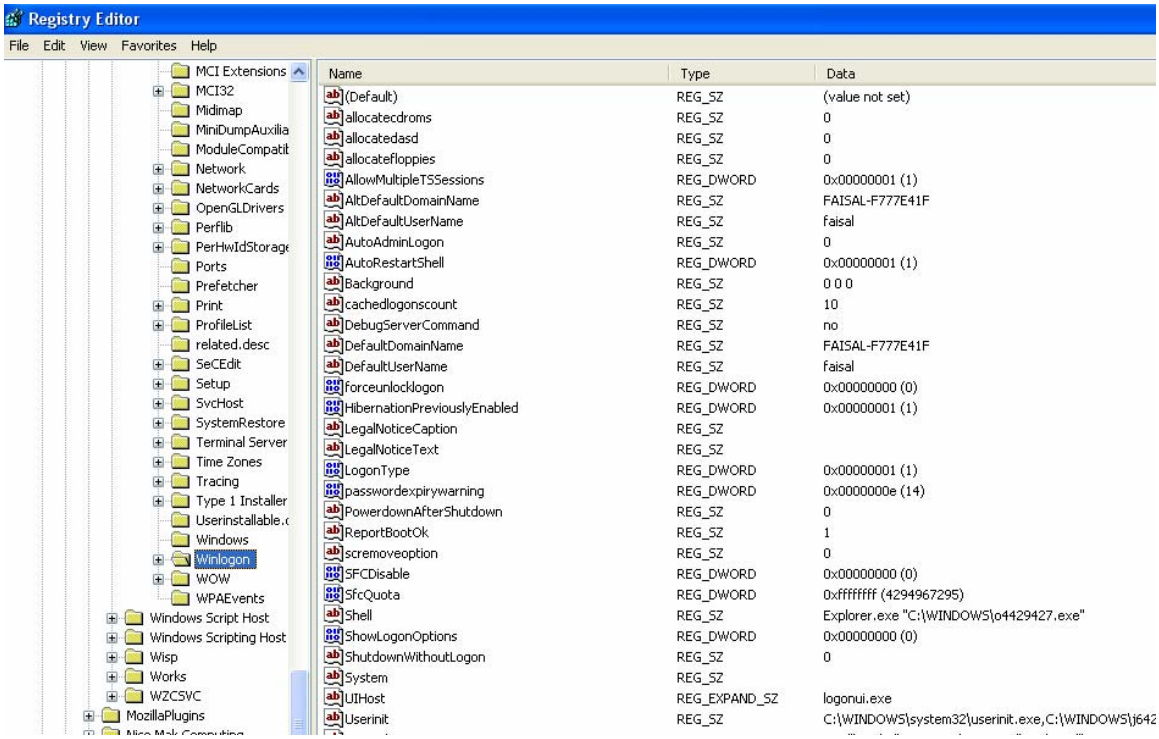


Open your regedit
Start->run->regedit



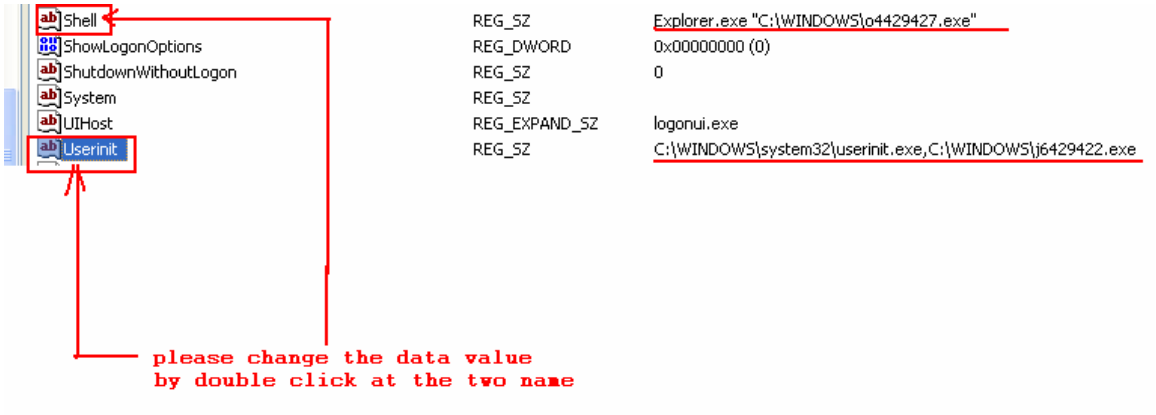
Then press ok button..

Ok.. please goto this key
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

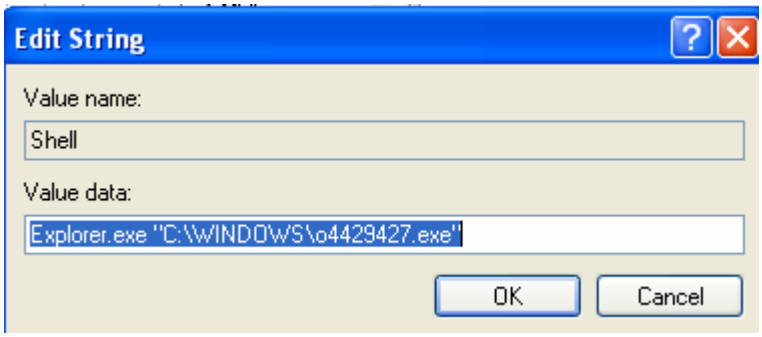


The tricky have been reveal..

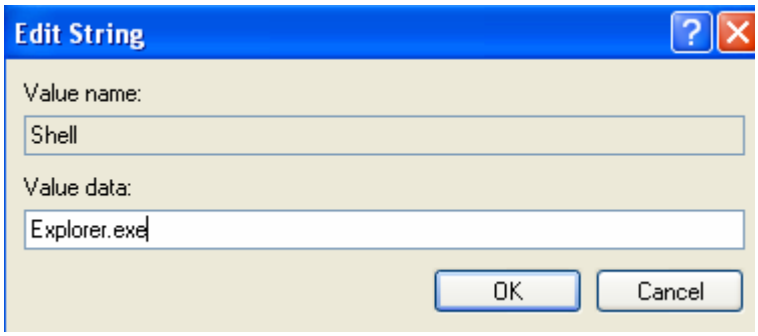
Look at the name field..
2 method to make the w0rm run after windows start
Look at Shell and Userinit



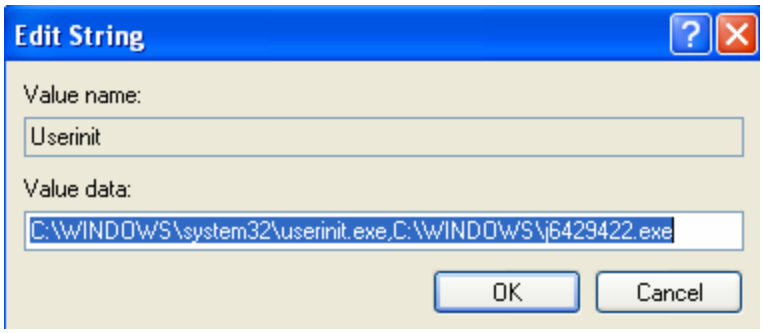
Double click at Shell



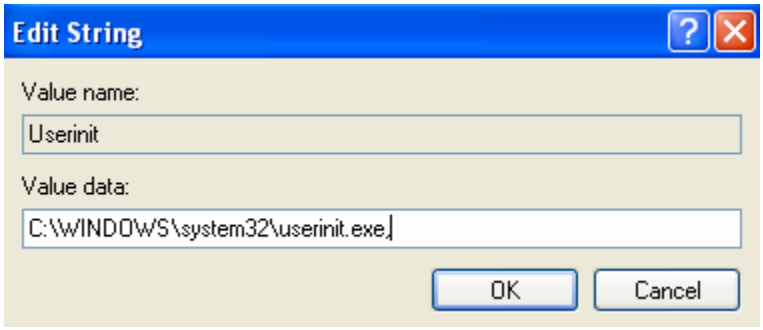
And delete the "C:\WINDOWS\o4429427.exe" ← random value due to make it confuse the cleaner..
Make sure it just Explorer.exe



Double Click at Userinit

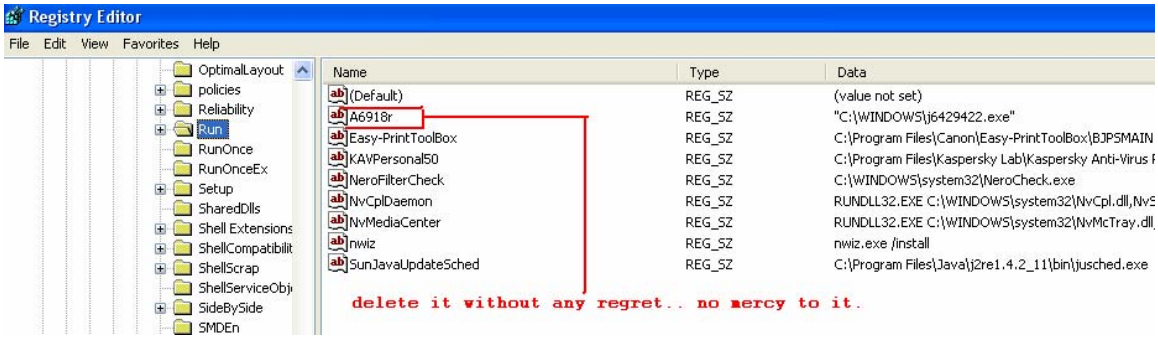


Delete the C:\WINDOWS\j6429422.exe <- random again



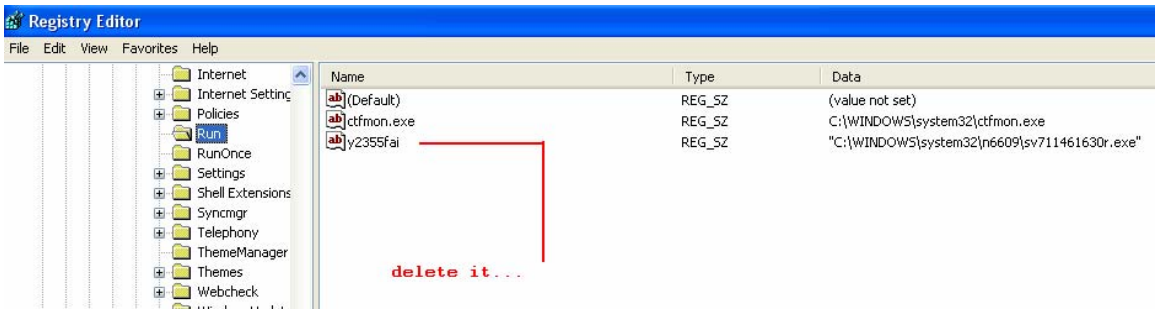
And press OK

Ok
Look at this key
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Find the unintelligible name



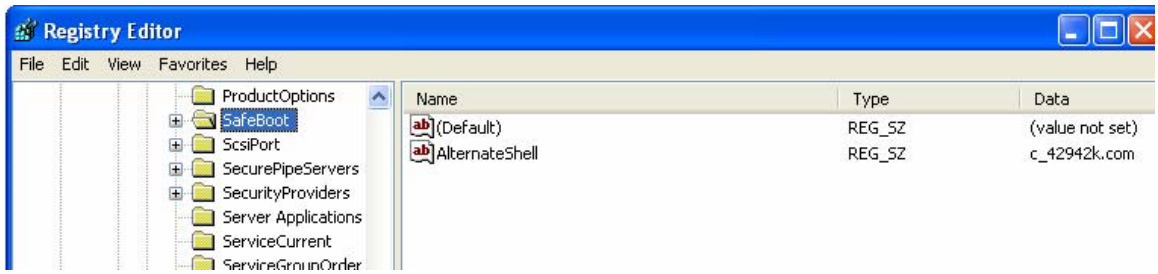
Look at this key

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

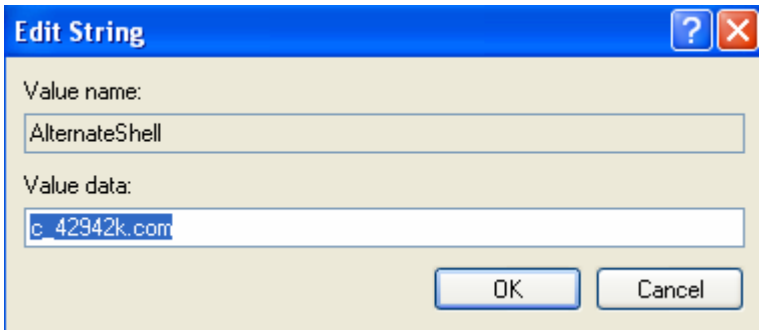


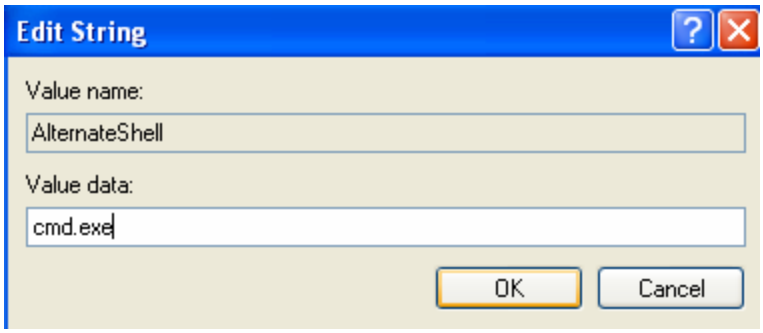
Then look at this key

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot

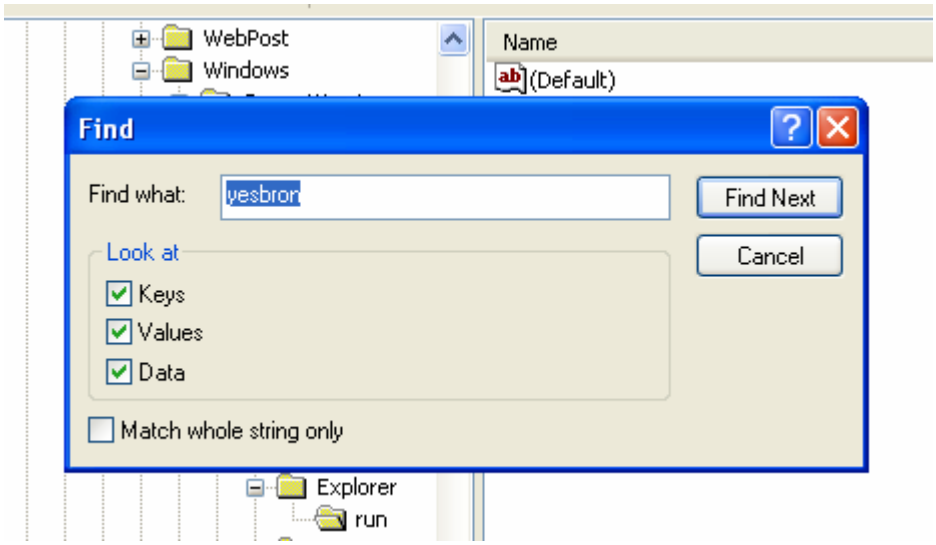


Double Click at the AlternateShell then Change c_42942k.com to cmd.exe





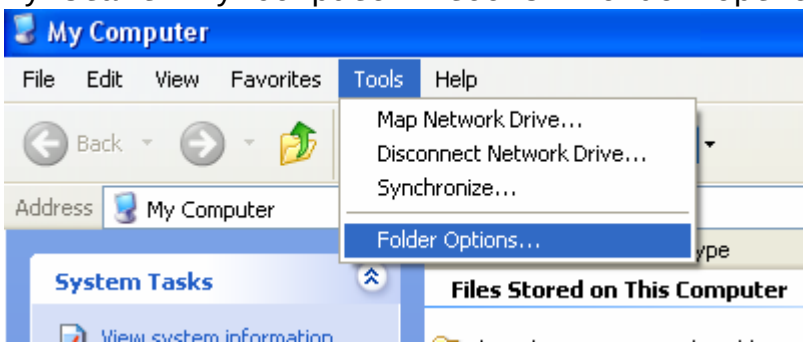
Please press F3 to find yesbron

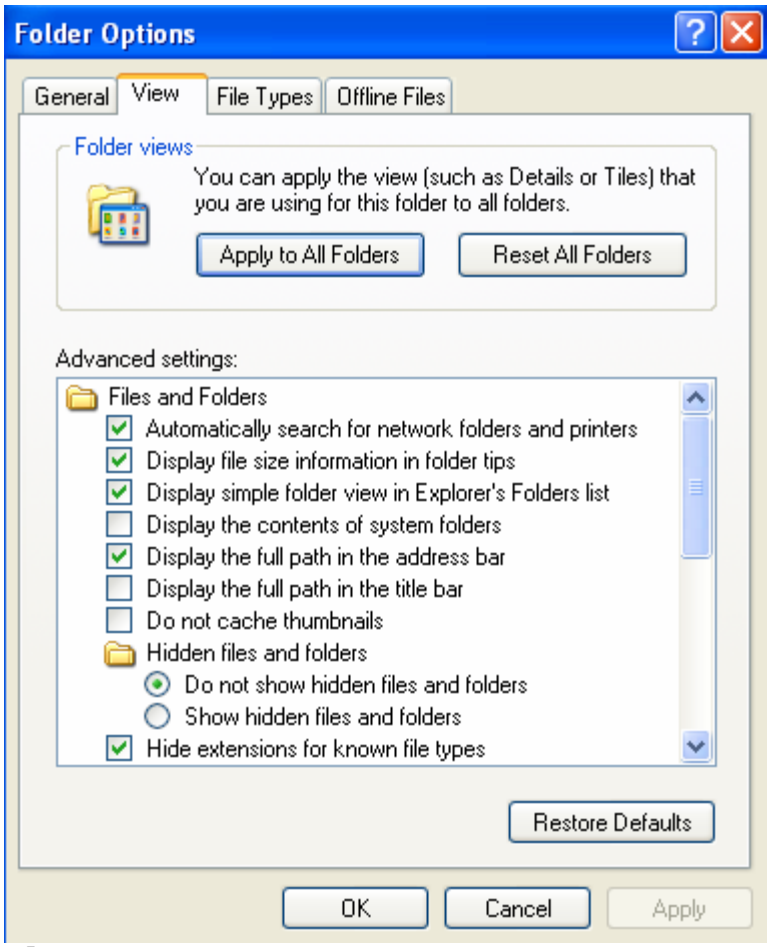


If you find it please delete it..

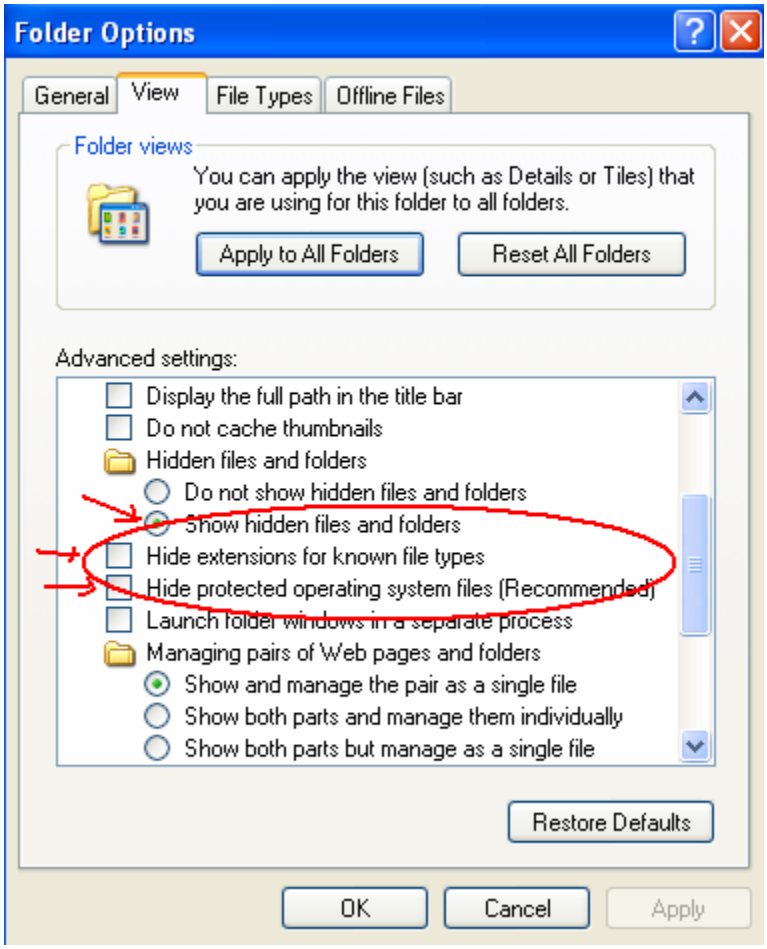
Ok... let find the file of rontokbro..
Now you can open any folder.. please setting your folder option

By start->My Computer->tools->folder option



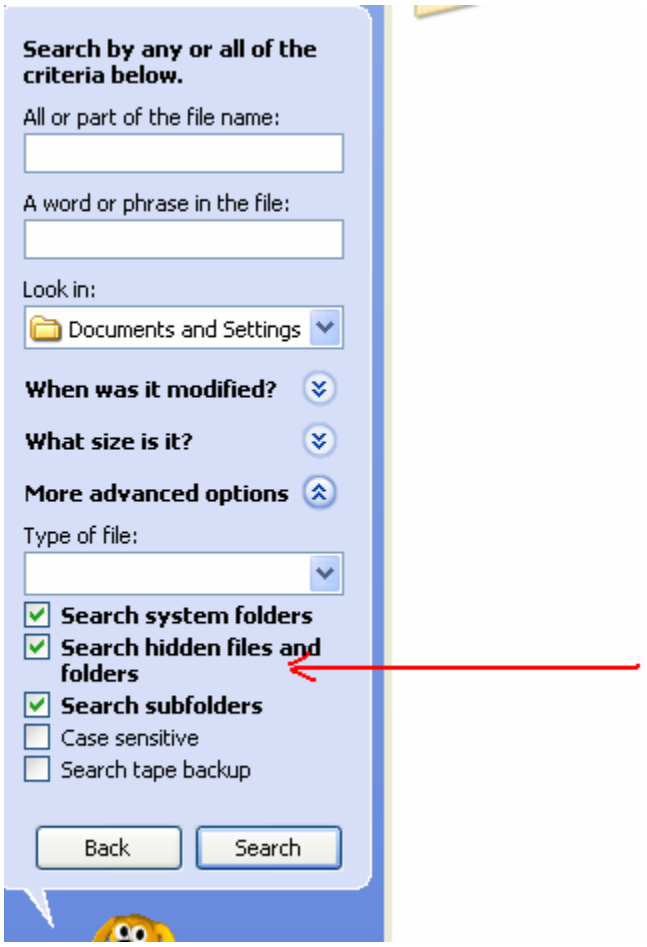


Please check the radio buton of Show Hidden files and folders

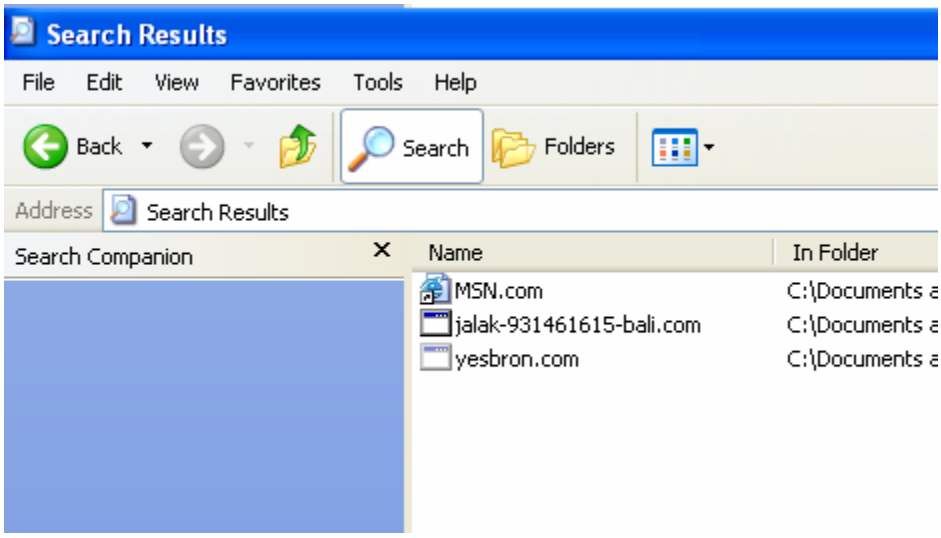


Please uncheck the “hide extensions for known file types”
And uncheck “hide protected operation system files”

Go to C:\Documents and Settings
Then make a setting at search option



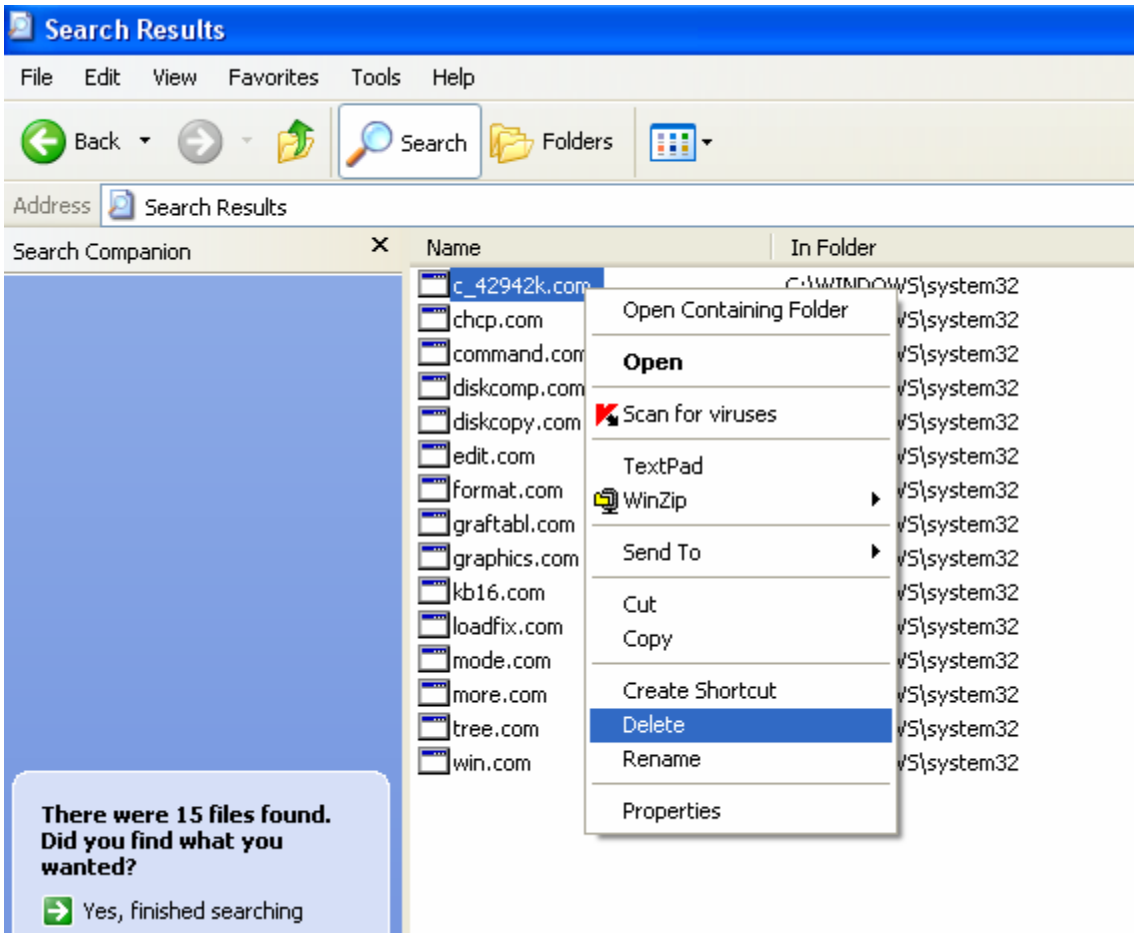
Please search for “*.com” without quote



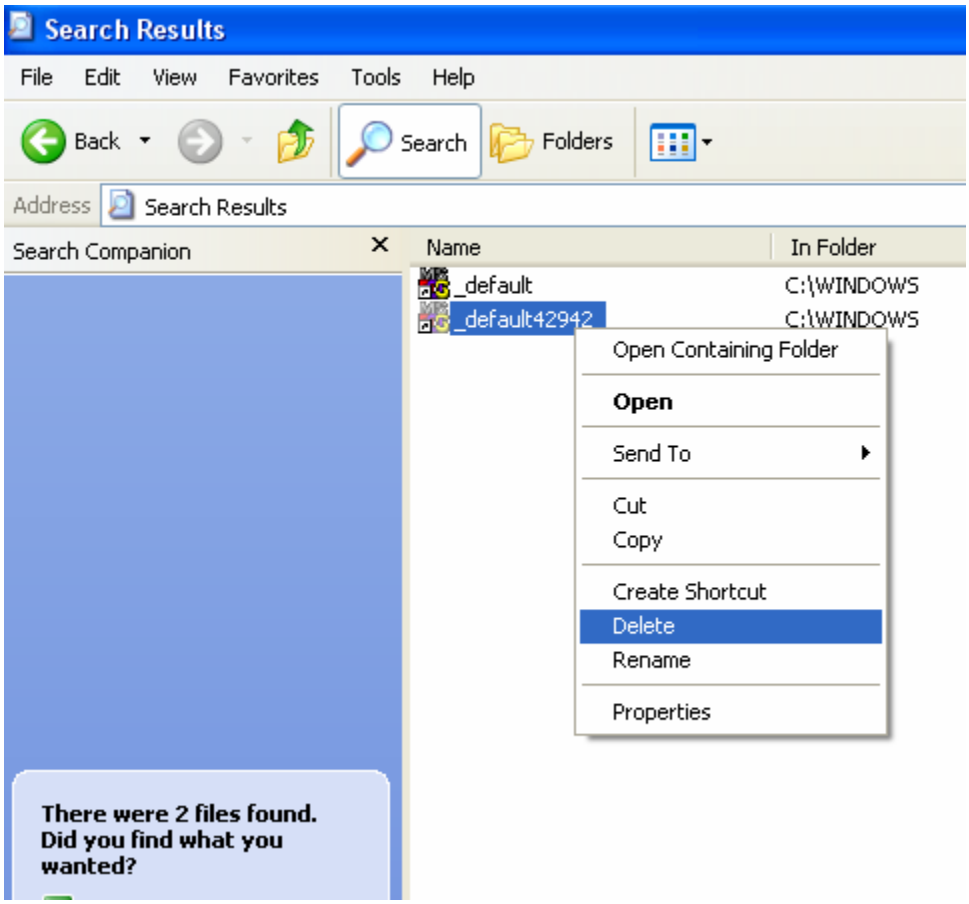
If you find it.. please delete it...

Goto C:\WINDOWS

Please search for *.com
You will get c_42942k.com < I think it’s random..
Delete it..

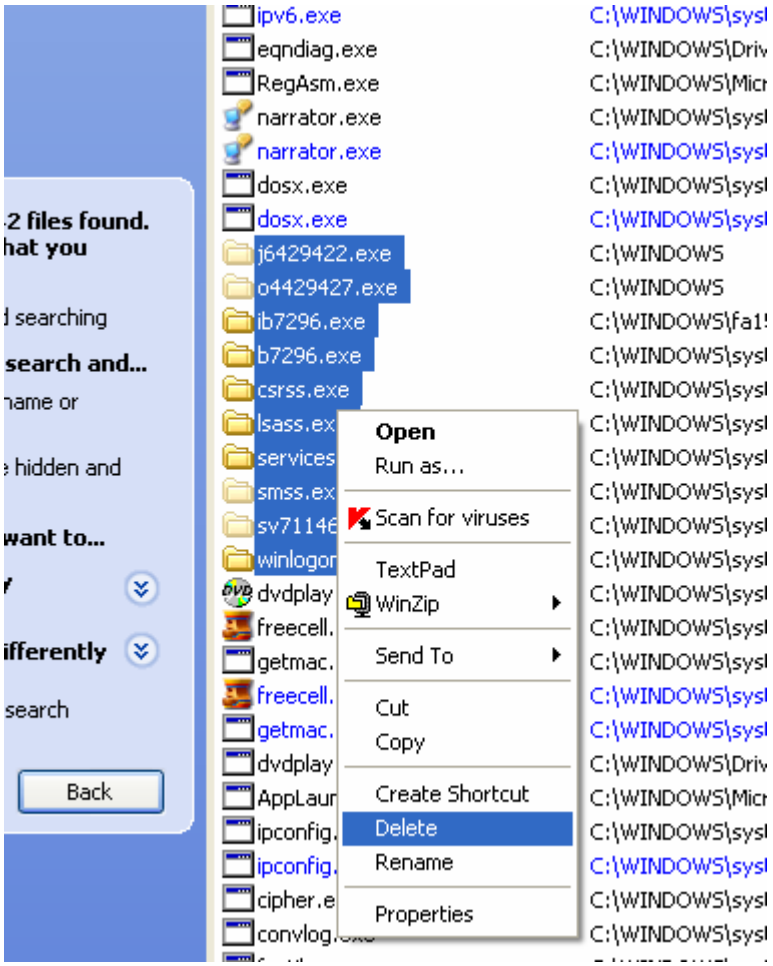


Ok search for *.pif



You will get _default42942.. delete it..

Find *.exe



The *.exe with the same characteristic
It has the folder’s icon.. delete them

ok.. that all... please install system mechanic to repair your registry.. ok.. good Luck

ok… my flu going worst..

Thanks Allah for give me the solution

Greets: F A,Asmah .. Perghh I’m so lazy ..anybody who know me .. that equal ;p