Relevant Knowledge: what is it, how it get installed and how to remove it

Already few days have passed since the **Relevant Knowledge** globe sits there in the *taskbar* in *Notification area*. I was very busy the last few days and I don't give too much attention to it but today looking at it, I start to ask myself how this globe got there? I don't remember to got installed anything with that name, Relevant Knowledge for sure a *parasitic* program and I decided to track back, what program carried it on? Because in my opinion, to install something in a computer without its owner knowledge or agreement is highly immoral and unethical, even more is very dangerous. It's a logical flow of thoughts, why to hide the actions performed by a program or if it installs something more in the computer, that's because these extra programs are not desirable by the user or malevolent. We know a lot about computer programs that comes with adware or spyware components embedded, beeing a real threat to the user privacy, in fact a real threat to his *cyber-life*.

I compare the computer with a virtual home, nobody wants to live in the house with someone sitting under the bed spying all of his movements and waiting for the right time to break the safe-box for example. I'm not exagerating, I know things like compromised email or online banking accounts happens all the time despite the users thinks they are fully impenetrable protected. As a matter of fact this is the biggest danger, to think you are 100% protected, it does not matter what antivirus solution you run.

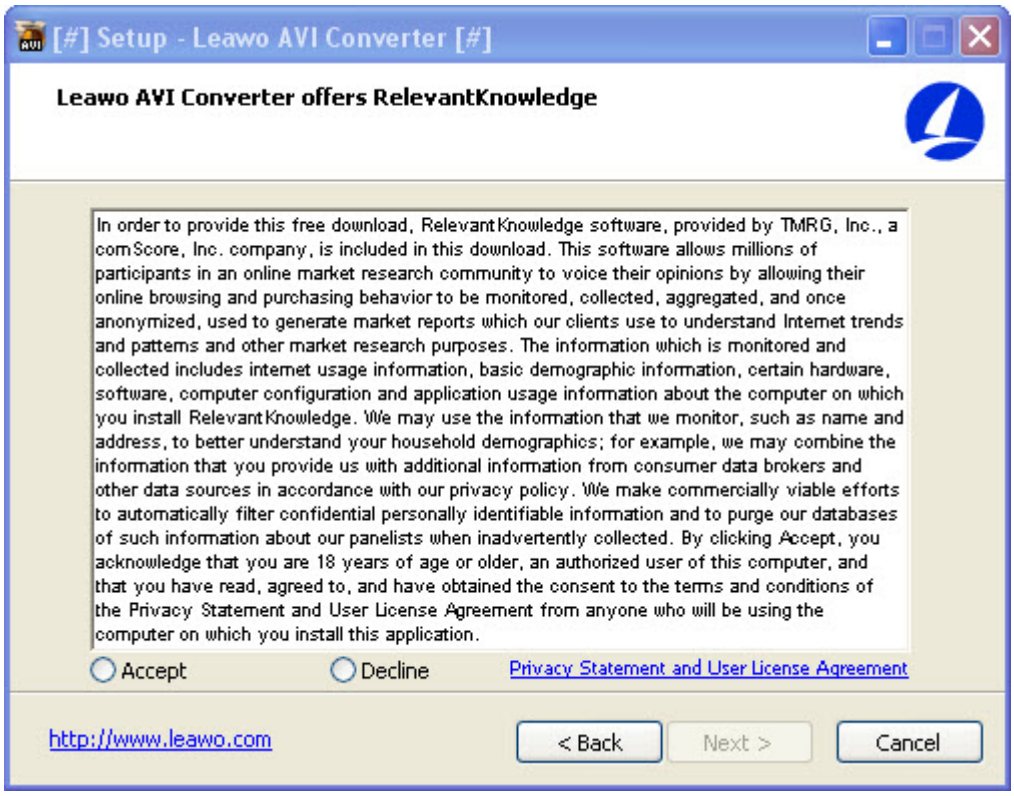
I was very curious what program was piggybacking this misterious program Relevant Knowledge so I started to look in *Program Files* directory for the program installation folder and its *creation date*. It was created several days ago somebody asked me to make a wmv file playable on a PS3 and I was testing some freeware video converters. Looking for files(in Temp directory, Program Files directory, Temporary Internet Files) with a creation date close to the Relevant Knowledge folder, all the tracks was leading to **Leawo Free AVI Converter** as the main suspect so I reinstalled it this time sandboxed and monitoring all the actions performed by the program. To achieve this I've used **Sandboxie** with **BSA** add-on, my favourite tools for analysis.

When the installation started :

two folders appears in the *%currentuser%\Local Settings\Temp* directory, one containing a file *avi2video_install.tmp* and the other 3 files :

- rkverify.exe -268 KB -Company: TMRG, INC. -MD5: 020CE95075F8C93E6CC957953D7F4589
- LogFile.dll -227 KB
- EncStr.dll -397 KB

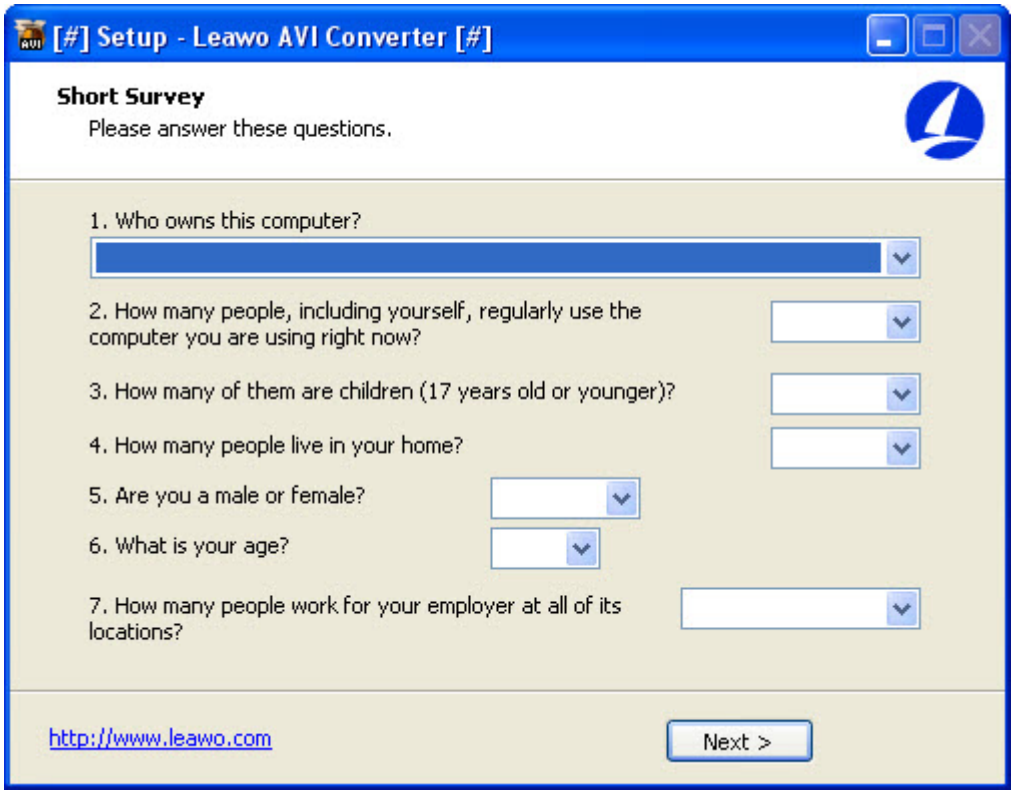
The next screen is a message about offering Relevant Knowledge software :



So there is a message about installing Relevant Knowledge, therefore I can not say its installation is

hidden but simply when I installed first time the video converter, I did not pay too much attention to this window. It's a learned lesson, always take the time to read carefully the messages and License Agreement preceding a software installation. I'm sure my mistake is very common amongst the computer users.

After the License Agreement and the installation procedure a short survey was following :



and the Relevant Knowledge program start to act. There is a long list of URLs where the program connects some of them very weird and scaring because I saw the program connecting to some of the sites where I was logged in before:

[Network services]
* Looks for an Internet connection.
* Backdoor functionality on port 0.
* Connects to "post.securestudies.com" on port 80.
* Connects to "165.193.78.234″ on port 443.
* Connects to "91.209.196.174″ on port 80.
* Connects to "" on port 80.
* Connects to "127.0.0.1″ on port 6323.
* Connects to "www.relevantknowledge.com" on port 80.
* Connects to "165.193.78.245″ on port 80.
* Connects to "165.193.78.234″ on port 80.
* Connects to "oss-content.securestudies.com" on port 80.
* Connects to "66.119.33.170″ on port 80.
* Connects to "insider.msg.yahoo.com" on port 80. <== The program connects to yahoo.com in my account maybe???
* Connects to "67.195.186.236″ on port 80.
* Connects to "217.146.187.123″ on port 443.
* Connects to "93.184.220.29″ on port 80.
* Connects to "www.whatismyip.com" on port 80.

* Connects to “72.233.89.199″ on port 80.
* Connects to “cnfg.facemoods.com” on port 80.
* Connects to “70.38.71.104″ on port 80.
* Connects to “xxxxx.com” on port 80. <== here was one of my sites where I was logged in before.Why it connects there ???And how, maybe using the saved cookies ?
* Connects to “46.102.241.179″ on port 80.
* Connects to “www.dvd-ppt-slideshow.com” on port 80.
* Connects to “173.244.164.35″ on port 80.
* Connects to “cleanbytes.net” on port 80. <== you can see here the program connects to this site cleanbytes.net, but why and how?
* Connects to “173.193.32.144″ on port 80.
* Connects to “player.play.it” on port 80.
* Connects to “81.196.26.161″ on port 80.
* Connects to “www.leawo.com” on port 80.
* Connects to “www.google.com.tr” on port 80.
* Connects to “74.125.87.104″ on port 80.
* Connects to “cdn-aws.mywot.net” on port 80.
* Connects to “216.137.61.67″ on port 80.
* Connects to “www.mywot.com” on port 80.
* Connects to “217.149.52.196″ on port 80.

According to Sandboxie add-on BSA, the software enumerates the running processes, enable process privileges and has keylogger functionality. Also the program creates a lot of processes and mutexes :

Created an event named: CS_CONFIDENCE_COMPLETE
Created an event named: DisableLowDiskWarning
Created an event named: MSCTF.SendReceive.Event.EMP.IC
Created an event named: MSCTF.SendReceive.Event.IEB.IC
Created an event named: MSCTF.SendReceive.Event.INK.IC
Created an event named: MSCTF.SendReceiveConection.Event.EMP.IC
Created an event named: MSCTF.SendReceiveConection.Event.IEB.IC
Created an event named: MSCTF.SendReceiveConection.Event.INK.IC
Created an event named: OSSListening
Created an event named: OSSProxyShutdownEvent
Created an event named: OSSProxyUpgradeEvent
Created an event named: OSSProxyUpgradeMenuEvent

……

Created process: (null),netsh firewall add allowedprogram program = “c:\program files\relevantknowledge\rlvknlg.exe” name = rlvknlg.exe mode = ENABLE scope = ALL,(null) <== add a rule to the firewall
……

Defined registry AutoStart location added or modified:
machine\software\Classes\clsid\{083863F1-70DE-11D0-BD40-00A0C911CE86}\Instance\{64697678-0000-0010-8000-00AA00389B71}\CLSID = {64697678-0000-0010-8000-00AA00389B71}
Defined registry AutoStart location added or modified:
machine\software\Classes\clsid\{083863F1-70DE-11D0-BD40-00A0C911CE86}\Instance\

{64697678-0000-0010-8000-00AA00389B71}\FilterData = ...

Defined registry AutoStart location added or modified:
user\current\software\Microsoft\Windows\CurrentVersion\RunOnce\OSSProxy =
c:\program files\relevantknowledge\rlvknlg.exe -bootinstall
Detected backdoor listening on port: 0
Detected keylogger functionality
Detected process privilege elevation
Enumerated running processes
IE settings change: user\current\software\microsoft\internet
explorer\main\windowssearch\version = ws not installed

.....
Opened a service named: LanmanServer
Opened a service named: NapAgent
Opened a service named: RASMAN
Opened a service named: RemoteAccess
Opened a service named: Router
Opened a service named: Sens

Risk evaluation result: High

To do its job, the software use a proxy named *OSS proxy*, to disable it seems to be enough to delete this registry key :

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\OSSProxy

The installation directory contained 2 files:

***rlvknlg.exe** by TMRG, INC. -MD5 983021B2913EA68DA2E4F0FC9E09A8AB

and

***rlservice.exe** by TMRG, INC. MD5 4B2D9D2DD644BE510E9AC7121EDD6D71

Disassembling rlvknlg.exe with IDA Pro Disassembler reveal other interesting facts :

.rdata:005EE82C aActivityLoadho db 'Activity::LoadHookDLL: (%d) %s',0Dh,0Ah,0
.rdata:005EE82C ; DATA XREF: sub_4046E9+1A0o
.rdata:005EE84D align 10h
.rdata:005EE850 ; char aActivityEnable[]
.rdata:005EE850 aActivityEnable db 'Activity: Enabled keyboard hooks (%p)',0Dh,0Ah,0
.rdata:005EE850 ; DATA XREF: sub_4048CB+A9o
.rdata:005EE878 ; char aActivityEnab_0[]
.rdata:005EE878 aActivityEnab_0 db 'Activity: Enabled mouse hooks (%p)',0Dh,0Ah,0
.rdata:005EE878 ; DATA XREF: sub_4048CB+D8o
.rdata:005EE89D align 10h
.rdata:005EE8A0 ; char aActivityEnab_1[]
.rdata:005EE8A0 aActivityEnab_1 db 'Activity: Enabled shell hooks (%p)',0Dh,0Ah,0
.rdata:005EE8A0 ; DATA XREF: sub_4048CB+107o
.rdata:005EE8C5 align 4

.rdata:005EE8C8 ; char aActivityEnab_2[]
.rdata:005EE8C8 aActivityEnab_2 db 'Activity: Enabled message hooks (%p)',0Dh,0Ah,0
.rdata:005EE8C8 ; DATA XREF: sub_4048CB+136o

.....

char aSkypecontrol_0[]
.rdata:005E3174 aSkypecontrol_0 db 'SkypeControlAPIAttach',0 ; DATA XREF:
sub_579CF1+18o
.rdata:005E318A align 4
.rdata:005E318C ; char aSkypecontrolap[]
.rdata:005E318C aSkypecontrolap db 'SkypeControlAPIDiscover',0 ; DATA XREF:
sub_579CF1+8o
.rdata:005E31BC aSkype_exe db 'Skype.exe',0 ; DATA XREF: sub_57A140+7Co
.rdata:005E31C6 align 4
.rdata:005E31C8 aGetCurrentuser db 'GET CURRENTUSERHANDLE',0 ; DATA XREF:
sub_57AAB0+4Fo
.rdata:005E31DE align 10h
.rdata:005E31E0 ; char aActivemembers[]
.rdata:005E31E0 aActivemembers db ' ACTIVEMEMBERS ',0 ; DATA XREF:
sub_57AB35+5DCo
.rdata:005E31E0 ; sub_57AB35+6CCo ...
.rdata:005E31F0 ; char aChat[]
.rdata:005E31F0 aChat db 'CHAT ',0 ; DATA XREF: sub_57AB35+5C4o
.rdata:005E31F0 ; sub_57AB35+6B0o
.rdata:005E31F6 align 4
.rdata:005E31F8 aGetChat db 'GET CHAT ',0 ; DATA XREF: sub_57AB35+526o
.rdata:005E3202 align 4
.rdata:005E3204 aActivemember_0 db ' ACTIVEMEMBERS',0 ; DATA XREF:
sub_57AB35+513o
.rdata:005E3213 align 4
.rdata:005E3214 aChatname_1 db 'CHATNAME ',0 ; DATA XREF: sub_57AB35+4E3o
.rdata:005E321E align 10h
.rdata:005E3220 ; char aChatname_0[]
.rdata:005E3220 aChatname_0 db 'CHATNAME',0 ; DATA XREF: sub_57AB35+4B2o
.rdata:005E3229 align 4
.rdata:005E322C aChatname db ' CHATNAME',0 ; DATA XREF: sub_57AB35+429o
.rdata:005E3236 align 4
.rdata:005E3238 aBody_1 db 'BODY ',0 ; DATA XREF: sub_57AB35+3CCo
.rdata:005E323E align 10h
.rdata:005E3240 aGetChatmessage db 'GET CHATMESSAGE ',0 ; DATA XREF:
sub_57AB35+2BBo
.rdata:005E3240 ; sub_57AB35+438o
.rdata:005E3251 align 4
.rdata:005E3254 aBody_0 db ' BODY',0 ; DATA XREF: sub_57AB35+2ACo
.rdata:005E325A align 4
.rdata:005E325C ; char aBody[]
.rdata:005E325C aBody db 'BODY',0 ; DATA XREF: sub_57AB35+1BCo
.rdata:005E3261 align 4
.rdata:005E3264 ; char aStatusSent[]
.rdata:005E3264 aStatusSent db 'STATUS SENT',0 ; DATA XREF: sub_57AB35+19Fo

.rdata:005E3270 ; char aMessage[]
.rdata:005E3270 aMessage db 'MESSAGE ',0 ; DATA XREF: sub_57AB35+181o
.rdata:005E3270 ; sub_57AB35:loc_57AD38o
.rdata:005E3279 align 4
.rdata:005E327C ; char aChatmessage[]
.rdata:005E327C aChatmessage db 'CHATMESSAGE ',0 ; DATA XREF:
sub_57AB35+168o
.rdata:005E327C ; sub_57AB35+1FCo
.rdata:005E3289 align 4
.rdata:005E328C ; char aCurrentuserhan[]
.rdata:005E328C aCurrentuserhan db 'CURRENTUSERHANDLE ',0
.rdata:005E328C ; DATA XREF: sub_57AB35:loc_57AC79o
.rdata:005E328C ; sub_57E557+53o
.rdata:005E329F align 10h
.rdata:005E32A0 aGetCall db 'GET CALL ',0 ; DATA XREF: sub_57AB35+C2o
.rdata:005E32AA align 4
.rdata:005E32AC aPartner_handle db ' PARTNER_HANDLE',0 ; DATA XREF:
sub_57AB35+AFo
.rdata:005E32BC ; char aInprogress[]
.rdata:005E32BC aInprogress db 'INPROGRESS',0 ; DATA XREF: sub_57AB35+36o
.rdata:005E32C7 align 4
.rdata:005E32C8 ; char aCall[]
.rdata:005E32C8 aCall db 'CALL ',0 ; DATA XREF: sub_57AB35+1Ao
.....

char aAdviewdataSe_0[]
.rdata:005EF150 aAdviewdataSe_0 db 'AdViewData::SendDataToServer, uploaded
screenshot to ad server.',0Dh
.rdata:005EF150 ; DATA XREF: sub_411294:loc_4118D7o
.....

char aInitializingBr[]
.rdata:005F19E0 aInitializingBr db 'Initializing BrowserMonitor',0Dh,0Ah,0

.rdata:005F1E08 aBrowsermoni_16 db 'BrowserMonitor: Checking %s,%s for survey
',0Dh,0Ah,0
.rdata:005F1E08 ; DATA XREF: sub_42BEFE+86o

aRequestid0x0_8 db 'RequestID 0x%08X: AOL traffic check %s (%s)',0Dh,0Ah,0
.rdata:005F40C0 ; DATA XREF: sub_435F72+416o
.rdata:005F40EE align 10h
.rdata:005F40F0 aConnectionEsta db 'Connection Established',0 ; DATA XREF:
sub_435F72+471o
.rdata:005F4107 align 4
.rdata:005F4108 ; char aRequestid0x0_9[]
.rdata:005F4108 aRequestid0x0_9 db 'RequestID 0x%08X: Live365 traffic check %s
(%s)',0Dh,0Ah,0

aTopspeed_pro_0 db 'topspeed.proxy.https',0 ; DATA XREF: sub_43940A+42Fo
.rdata:005F4DD1 align 4
.rdata:005F4DD4 ; char aSslTrafficForA[]
.rdata:005F4DD4 aSslTrafficForA db 'SSL traffic for AOL SE client will be tunnelled to

%s‘,0Dh,0Ah,0
.rdata:005F4DD4 ; DATA XREF: sub_43940A+49Co
.rdata:005F4E0C ; char aClientconne_21[]
.rdata:005F4E0C aClientconne_21 db ‘ClientConnectionThread 0x%08X, RTMP over port 80 detected.’,0Dh,0Ah,0
.rdata:005F63B0 aSurveyrulesurl db ‘SurveyRulesURL‘,0
.rdata:005F63BF align 10h
.rdata:005F63C0 aHttpRules_s_24 db ‘http://rules.securestudies.com/oss/rule1.asp’,0
.rdata:005F63ED align 10h
.rdata:005F63F0 aRemoteconfigur db ‘RemoteConfigURL’,0
.rdata:005F6400 aHttpRules_s_25 db ‘http://rules.securestudies.com/oss/rule16.asp’,0

.rdata:005F64F8 aMousetrackru_0 db ‘MouseTrackRulesURL‘,0
.rdata:005F650B align 4
.rdata:005F650C aHttpRules_s_29 db ‘http://rules.securestudies.com/oss/rule7.asp’,0
.rdata:005F6539 align 4
.rdata:005F653C aBiometricrul_3 db ‘BioMetricRulesURL‘,0
.rdata:005F654E align 10h
.rdata:005F6550 aHttpRules_s_30 db ‘http://rules.securestudies.com/oss/rule21.asp’,0
.rdata:005F657E align 10h
.rdata:005F6580 aLoggingrulesur db ‘LoggingRulesURL‘,0
.rdata:005F6590 aHttpRules_s_31 db ‘http://rules.securestudies.com/oss/rule3.asp’,0
.rdata:005F6E84 aDownloadedOsaF db ‘Downloaded OSA file from: %s‘,0
.rdata:005F6E84 ; DATA XREF: sub_442ACE+FBo
.rdata:005F9D80 aBankofamerica_ db ‘bankofamerica.com‘,0 ; DATA XREF: sub_469119+E2o
.rdata:005F9D80 ; sub_48AB66:loc_48B7EFo …

.rdata:005FE684 ; char aMailproxy[]
.rdata:005FE684 aMailproxy db ‘MailProxy’,0 ; DATA XREF: sub_491E88:loc_492A58o
.rdata:005FE684 ; sub_4A276C+7BAo
.rdata:005FE68E align 10h
.rdata:005FE690 ; char aEvsMailproxySe[]
.rdata:005FE690 aEvsMailproxySe db ‘EVS: MailProxy setting removed.’,0Dh,0Ah,0
.rdata:005FE690 ; DATA XREF: sub_491E88+BF6o
.rdata:005FE6B2 align 4
.rdata:005FE6B4 ; char aEvsErrorUnab_0[]
.rdata:005FE6B4 aEvsErrorUnab_0 db ‘EVS: Error – Unable to delete MailProxy setting!’,0Dh,0Ah,0
.rdata:005FE6B4 ; DATA XREF: sub_491E88+C27o
.rdata:005FE6E7 align 4
.rdata:005FE6E8 ; char aEvsMailproxy_0[]
.rdata:005FE6E8 aEvsMailproxy_0 db ‘EVS: MailProxy setting not found.’,0Dh,0Ah,0
.rdata:005FE6E8 ; DATA XREF: sub_491E88:loc_492AD9o
.rdata:005FE70C ; char aEvsDeletingAol[]
.rdata:00601098 aCachePoisonP_0 db ‘Cache Poison Ping: Successfully sent cache poison ping with url ‘
.rdata:00601098 ; DATA XREF: sub_4A4970+2ECo

.rdata:0060B6F0 aWininetrequ_10 db ‘WinInetRequest: Content-Type [%s]‘,0Dh,0Ah,0
.rdata:0060B6F0 ; DATA XREF: sub_507A72+39Fo

.rdata:0060B714 ; char aWininetrequ_11[]
.rdata:0060B714 aWininetrequ_11 db 'WinInetRequest: Read %d bytes',0Dh,0Ah,0
.rdata:0060B714 ; DATA XREF: sub_507A72+3DAo
.rdata:0060B734 asc_60B734: ; DATA XREF: sub_5BEDE0+59o

The list with procedures and functions used by Relevant Knowledge is long and just looking at them is scaring enough. The program seems to serve surveys and advertisement to the users along with closely spying their behaviour on the Internet. I don't know what to say more, I don't know who in all of his minds wants this program installed in the computer, so my advice is to get rid of it as quick as possible. I don't say Relevant Knowledge software steal some confidential informations from the computer users either I can not say it's a hidden install since there is a message at the beginning of installation(even wrote with small small letters) but seems to be ready for serving unwanted advertisements and surveys and it looks like a very high security risk for the users.

Uninstall it from the *Remove Programs* tab in *Control Panel*, delete all of the remaining files and folders from Program Files directory and clean the registry for all the remaining keys. How to do this ? Just use Process Explorer from Sysinternals, now microsoft.com and be sure no Relevant Knowledge components(OSS proxy, rlvknlg.exe, rlservice.exe, rlls.dll, rk.osa) are running and Autoruns to determine what programs and services run at start-up and delete all the references to Relevant Knowledge. Both are free, light and very efficient programs.

And, as a last recomandation, always take the time to read the messages preceding a program installation and you will not have nasty surprises. This program, **Leawo Free AVI Converter** is free as the title says but with what price ?

Keep safe !