The fake VLC Media Player and serious business

Sometimes, navigating on the Web we find a link to a very tempting video which are demanding a necessary plugin to play, or a special player or simply a codec. Maybe we receive this link in an email, or somebody(not a friend that's for sure) send it to us on Facebook or even we download a bogus video file which try to force us to download a certain player. No other player can play this video but especially that one. Well, this scenario is old and a lot used by evil persons or companies to trick us to run their malicious software.

Trojans? Viruses? Not necessary, but adware, software which spy on you and on your online habits, software which installs possible backdoors on your system, software which you normally avoid if you can because make you feel uncomfortable but is silently installed without your agreement.

Obviously, to increase the chances of this harmful content to be downloaded, bad coders use well known names. Who does not know about VLC Media Player, the universal and free player? These days was its turn to be counterfeited and a fake version is offered for download on several sites, these are a few:

> http://free-media-player.info/pluginplayer1/
>
> http://trusted-player.info/pluginplayer1/
>
> http://media-player-software.com/pluginplayer1/

If we introduce in browser URL address only *http://media-player-software.com* we see only the server Apache test page but if we add */pluginplayer1* we see this page offering the fake player for download:

fake_website

OK, let's see what this application does, I run it using Sandboxie with BSA Sandbox Analyzer add on for quick analysis.

The application with name *VLC_Player_Setup.exe* has 445 KB in size, way too little to be the real *VLC Player* and is digitally signed by **INSTALLER TECHNOLOGY CO.,** a Florida based company.

This is the first window:

GorillaPrice Engine Offer

You can see what is default checked, *Install GorillaPrice Offer Engine, Jsip browser enhancement and ActiveCollector data analyzer to improve my browser experience*. To improve my browser experience or to improve their sales, now that's the question.

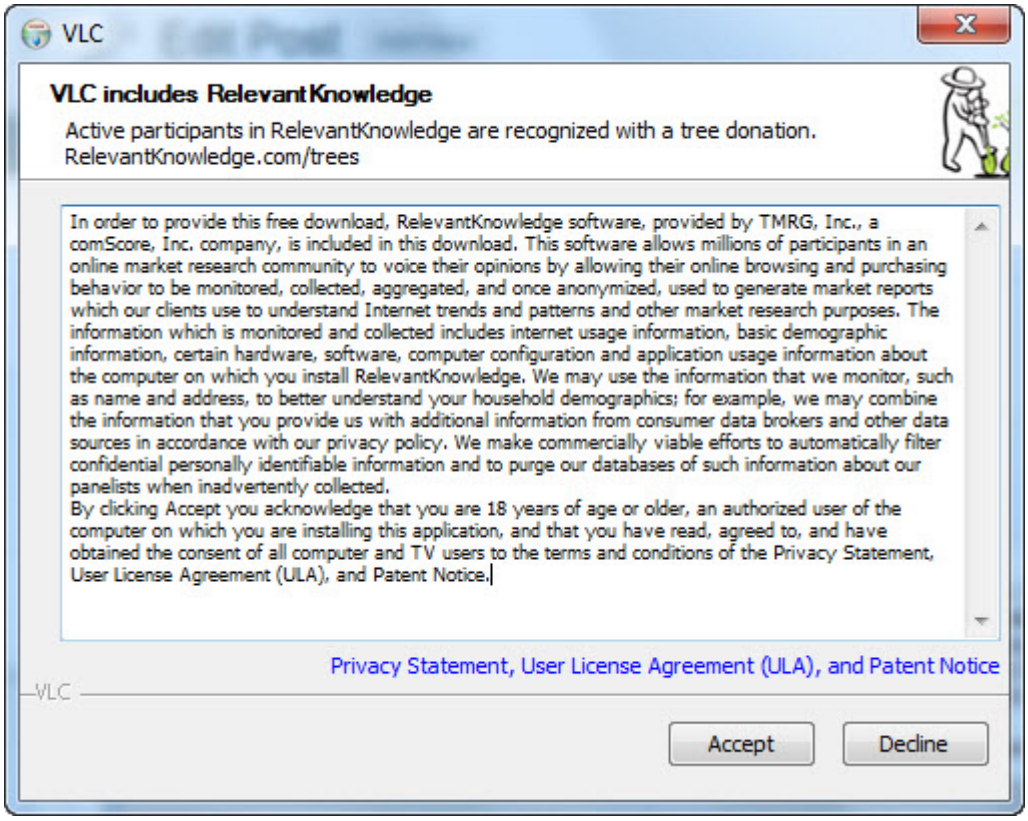
Strange, the application allowed me to uncheck the box and click Accept. The next window was this:

Babylon Toolbar offer

The boxes are unchecked by default but you can not move on without to check them, you have not the same luck like in the first offer with GorillaPrice Offer Engine. The *Next* button is disabled until you check them so you are forced to install *Babylon as homepage* and *Babylon search engine* , both of them if you want eventually to finish the installation and use VLC Media Player.

Next, the program made some connections and download something, we will see what later.

This is the next window:



VLC RelevantKnowledge

Whoops, the title is *VLC* and subtitle *VLC includes RelevantKnowledge*. The last time when I've checked VLC was a free and open source cross-platform multimedia player that does not carry any dubious "add on". At least you can click *Decline* and the program will finish its execution.

But just apparently the execution is finished, because in background remains running a process, *BrowserProtect.exe*, digitally signed by *Bit89 Inc*. I don't remember to install this one through the installation process. What it does? Nobody really knows but if you Google about *Bit89 Inc.* you will find that has a very bad reputation and the victims(can I say so?) are complaining about everyday pop-ups generated by temporary??? files and the publisher is *Bit89 Inc*. Not a desirable program in your PC anyway. On their official website, *www.bit89.com* it can be found an uninstaller for their program for who need it.

This an excerpt of the raport generated by *BSA sandbox analyzer*:

> .....
>
> [Network services]
> * Looks for an Internet connection.
> * Connects to "108.163.167.218″ on port 80.
> * Connects to "108.163.158.227″ on port 80.
> * Connects to "184.107.137.146″ on port 80.
> * Connects to "127.0.0.1″ on port 9876.
> * Connects to "127.0.0.1″ on port 52282.
> * Connects to "184.154.27.235″ on port 80.
> * Connects to "stp.babylon.com" on port 80.
> * Connects to "dl.babylon.com" on port 80.

* Connects to “216.104.42.91″ on port 80.
* Connects to “127.0.0.1″ on port 59670.
* Connects to “d1js21szq85hyn.cloudfront.net” on port 80.
* Connects to “54.240.162.226″ on port 80.
* Opens next URLs:

http://info.babylon.com/stat/report.php?no_policy=1&lang=0&source=setup-start&stage=0&ver=9.1.0.1&affilID=121266&guid={97FA19F9-56EF-4384-873D-B0AD9ABADDA9}&mntrId=6c8288df000000000000f8d1111ad39b&sufn=VLC_Player_Setup.exe&iev=8&ffv=18&crv=24&dwb=opera&wbr=7&sutp=50&sufl=66&tbp=0&prver=0&minreq=0&dtct=-10000000&wvr=601&tbtp=def&tbinst=1&cntry=US&uac=1&osp=hp0:-1938492880;hp1:0;hp2:0;dsp0:-886302982;dsp1:0;dsp2:-425396809;&dnt=2.0,3.0,3.5,4.0

http://info.babylon.com/stat/report.php?no_policy=1&lang=0&source=setup-start&stage=0&ver=9.1.0.5&affilID=121266&guid={D739BF15-46D8-4FEC-9BBF-F7E703125327}&mntrId=6c8288df000000000000f8d1111ad39b&hwid=6C82F8D1111AD39B&sufn=mybabylontb.exe&iev=8&ffv=18&crv=24&dwb=opera&wbr=7&dlb=uk&spb=cr&sutp=50&sufl=74&tbp=0&prver=0&minreq=0&dtct=-10000000&wvr=601&tbtp=def&tbinst=1&cntry=US&uac=1&osp=hp0:-1938492880;hp1:0;hp2:0;dsp0:-886302982;dsp1:0;dsp2:-425396809;&dnt=2.0,3.0,3.5,4.0

http://info.babylon.com/stat/report.php?no_policy=1&lang=0&source=setup-end&stage=90&ver=9.1.0.5&affilID=121266&trkInfo=[spt:1]&guid={D739BF15-46D8-4FEC-9BBF-F7E703125327}&mntrId=6c8288df000000000000f8d1111ad39b&hwid=6C82F8D1111AD39B&sufn=mybabylontb.exe&iev=8&ffv=18&crv=24&dwb=opera&wbr=7&dlb=uk&spb=cr&sutp=50&sufl=74&tbp=0&prver=0&minreq=0&dtct=-10000000&wvr=601&tbtp=none&tbinst=1&cntry=US&uac=1&osp=hp0:-1938492880;hp1:0;hp2:0;dsp0:-886302982;dsp1:0;dsp2:-425396809;&dnt=2.0,3.0,3.5,4.0&spbi=&CR2_sdsps&CR1_shps&hp=1&dsp=1&tb=1&hpx=1&dspx=1&tbx=0&dnld=100&dcnt=4&dtot=4&dlerr=200&rvrt=0&excd=3&stm=16&nvs=0&rbts=0&rbtt=0&ccp=0

http://info.babylon.com/stat/report.php?no_policy=1&lang=0&source=setup-end&stage=91&ver=9.1.0.1&affilID=121266&trkInfo=[spt:1]&guid={97FA19F9-56EF-4384-873D-B0AD9ABADDA9}&mntrId=6c8288df000000000000f8d1111ad39b&sufn=VLC_Player_Setup.exe&iev=8&ffv=18&crv=24&dwb=opera&wbr=7&sutp=50&sufl=66&tbp=0&prver=0&minreq=0&dtct=-10000000&wvr=601&tbtp=def&tbinst=1&cntry=US&uac=1&osp=hp0:-1938492880;hp1:0;hp2:0;dsp0:-886302982;dsp1:0;dsp2:-425396809;&dnt=2.0,3.0,3.5,4.0&hp=1&dsp=1&tb=1&hpx=0&dspx=0&tbx=0&dnld=100&dcnt=1&dtot=2&dlerr=200&rvrt=0&excd=0&stm=21&nvs=0&rbts=0&rbtt=0

[Process/window/string information]
* Enables process privileges.
* Gets user name information.
* Gets computer name.
* Checks for debuggers.
* Installs a hook procedure that monitors mouse messages.
* Checks if user is admin.
* Uses a pipe for inter-process communication.
* Deletes activity traces.
* Creates process “(null),C:\Program Files\i_technology\mybabylontb.exe /mtb=512 /mhp=512 /mnt=512 /mds=512 /babTrack=”affID=121266″ /s /aflt=babsst /instlRef=sst /srcExt=ss,(null)”.

* Injects code into process “c:\sandbox\cyberstorm\defaultbox\drive\c\program files\i_technology\mybabylontb.exe”.
* Creates process “(null),”C:\Users\CYBERS~1\AppData\Local\Temp\8254A48E-BAB0-7891-ACDD-B3C508BB6E74\Setup.exe” -uiname=babtb1 Files\i_technology\mybabylontb.exe” /mtb=512 /mhp=512 /mnt=512 /mds=512 /babTrack=”affID=121266″ /s /aflt=babsst /instlRef=sst /srcExt=ss,C:\Users\CYBERS~1\AppData\Local\Temp\8254A48E-BAB0-7891-ACDD-B3C508BB6E74\”.
* Injects code into process “c:\sandbox\cyberstorm\defaultbox\user\current\appdata\local\temp\8254a48e-bab0-7891-acdd-b3c508bb6e74\setup.exe”.
* Creates a mutex “Local\!IETld!Mutex”.
* Lists all entry names in a remote access phone book.
* Opens a service named “rasman”.
* Opens a service named “Sens”.
* Creates a mutex “IESQMMUTEX_0_208″.
* Enumerates running processes.

…….

Here is the analysis of the fake VLC player installer, detection ratio: **1 / 45**, at this time only DrWeb detect it as *Adware.Downware.885*.

BrowserProtect.exe by Bit89 company, which remains running in background after you finish the installation process, has a detection ratio of **9/45** here, with various labels: *Backdoor.Win32.Rbot.kur* by Kaspersky, *TROJ_SPNR.0BBC13* by TrendMicro or *a variant of Win32/bProtector.A* by NOD32. Again, not something desirable in your PC.

The funny part is that during this installation process, the real VLC Media Player is downloaded and installed so the victim is tricked until to the end, he will see the shortcut of VLC Player on his desktop and its files installed in Program Files folder and think that all its OK.

No, it’s not OK to fill your computer with rubbish, read harmful content because that is in fact adware, when you simply can download the real VLC Player from its official website, simple and without headaches.

In reality is all about money, the creator of the rogue VLC Player installer is an affiliate of *Babylon* company and of a few others and that’s is how he understand to increase his revenues, tricking the victims, installing potentially harmful software without the user consent, infecting people’s computers, that’s how he understands the serious business. Does Babylon company knows **how** its affiliates is spreading its software and how its reputation is affected? Maybe yes, maybe not or maybe it does not care, just another way to do business.

But when is all about money, there is no privacy or anonymity, there is no morality and the world become a jungle…

Things to check:

A website offering another fake VLC Media Player :
http://www.downloaddirect.com/software/vlc-player/2567

Fake VLC App appears in the Windows Store

Another Fake VLC for Windows 8 App Available for Download

Keep safe!

Share this:

- Share