How to completely remove W32.UsbFakeDrive Virus on computer and USB

The W32.UsbFakeDrive virus is a dangerous malware that can spread via USB and hide data. When users click on the fake shortcut, the virus will spread to the computer. To completely remove this threat, you need to use antivirus software combined with FixAttrb Bkav to restore hidden data.

The W32.UsbFakeDrive virus hides data on USB drives and can infect computers when accessing fake shortcuts. Proper scanning and removal of the virus helps protect data and prevent the risk of spreading.

Remove Virus W32.UsbFakeDrive

This type of virus is very dangerous to computers, not only does it hide data, it also brings many other dangers.

Some anti-virus software can detect and notify that the virus has been removed, but because the computer was previously infected with a virus, when we plug in the USB to use it, the virus still appears and the data in the USB is still hidden.

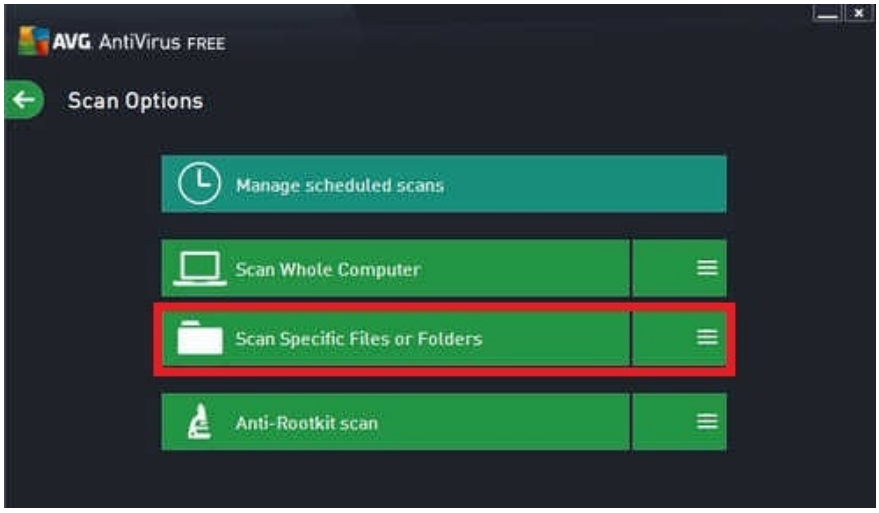
To kill this virus, we have to follow 2 steps: kill it on the computer and kill it on the USB, then use BKAV's FixAttrb application to show the files in the USB.

Remove W32.UsbFakeDrive Virus on Computer, on USB

- Download the latest version of AVG Free Antivirus (currently AVG Free 2014). Install the software on your computer, after installation, restart your computer.

- From the main interface of AVG 2014 program, select **?** as shown below.

- In this step, select **Scan Spectific Files or Folders**



- In this step, we select the drives to scan (in this case, drive **C:** , **drive D:** and USB drive is drive **G:**), then we select **Startscan**

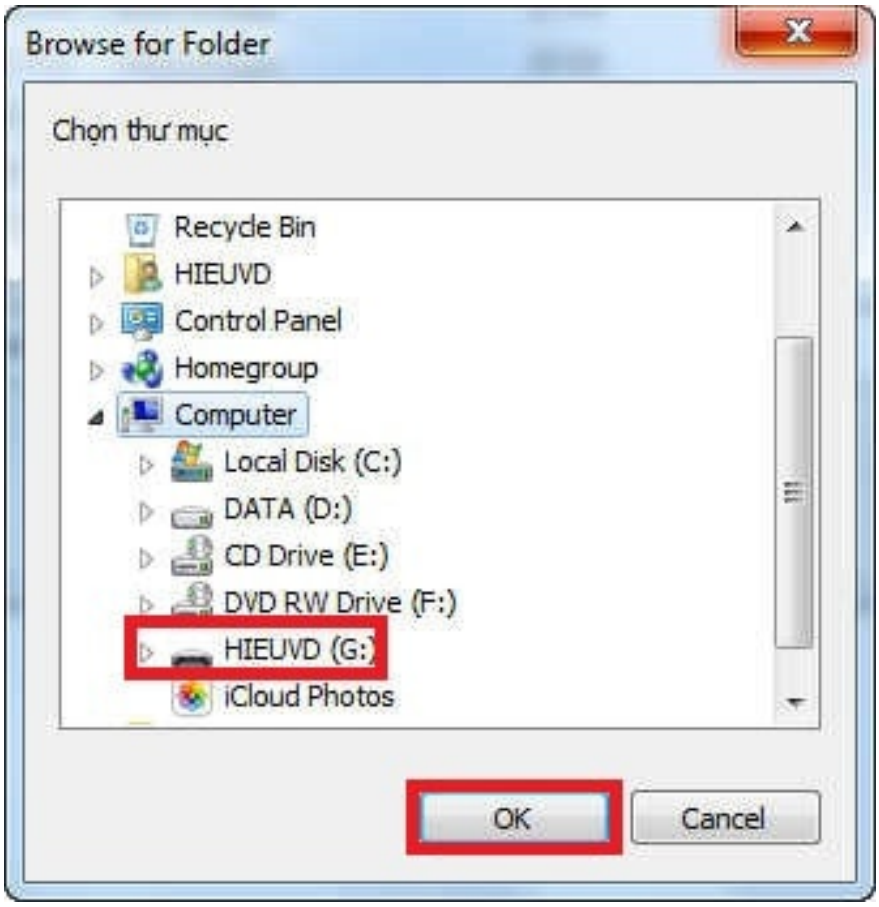
- After scanning, we use the **FixAttrb** application to display the data.

Use BKAV's FixAttrb application to display data in USB

- Download FixAttrb app here

- Double click on **FixAttrb.exe** , select **Select drive** .

- In this step, we select the USB drive (in this case, drive G:), then select **OK** and access the USB to use our data.



The W32.UsbFakeDrive virus is a dangerous malware that usually infects USB and can hide data on removable drives. When users open the fake shortcut of the USB, the virus will activate and spread to the computer, causing the risk of data loss. To completely remove it, you need to scan for viruses on both the computer and the USB, then use the hidden file recovery tool to retrieve the data. In addition, turn off the AutoRun feature on Windows to limit virus penetration from mobile devices.

You finished reading the article "**How to completely remove W32.UsbFakeDrive Virus on computer and USB**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
