Remove Smart HDD (Uninstall Guide)

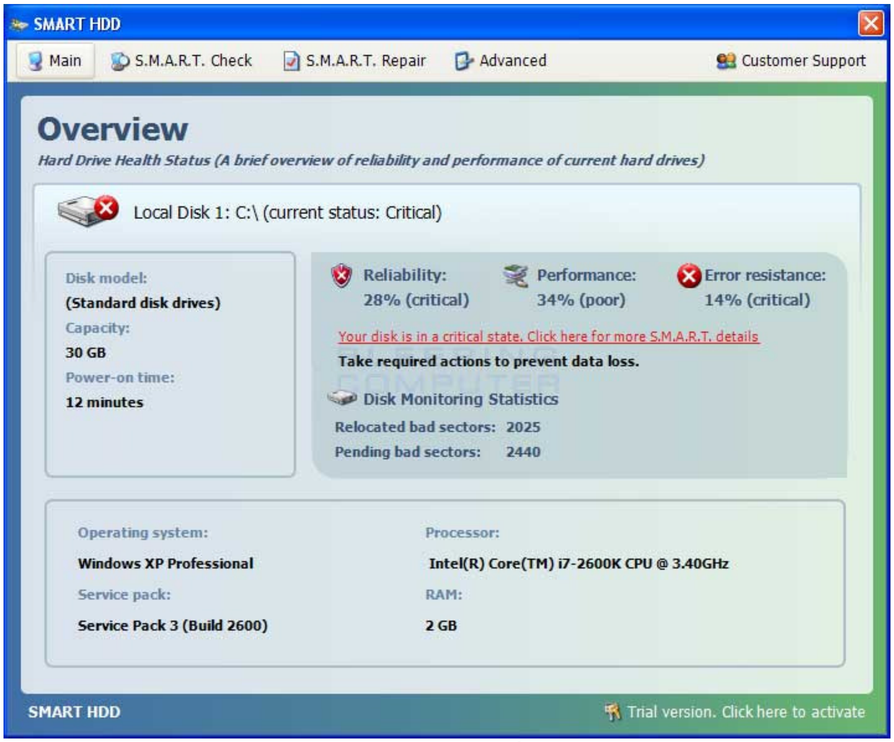
Posted by Lawrence Abrams on December 14, 2010 @ 01:37 PM · Views: 181,074

Smart HDD is a fake hard drive optimization and analysis program that displays false information so that it can scare you into thinking that there is something wrong with your computer's hard disks. This program is part of the Rogue.FakeHDD family of scareware programs. Smart HDD is installed via Trojans that display fake error messages on the infected computer. These messages will state that there is something wrong with your computer's hard drive in order to scare you into purchasing the program.

Once installed, Smart HDD will be configured to start automatically when you login to Windows. Once started, it will pretend to perform a **S.M.A.R.T. Check** routine that supposedly examines your hard drive for S.M.A.R.T. errors. When it has finished it will present you with a **S.M.A.R.T. Repair** screen where it will display a fake hard drives diagnostic report. This report will state that there are numerous issues with your computer's hard disks and then prompt you to repair these issues. If you attempt to repair any of these issues, though, it will first state that you need to purchase a license. Some examples of the fake problems that it will report are:

Hard drive boot sector reading error
System blocks were not found
Error 0x00000024 - NTFS_FILE_SYSTEM
Error 0x00000078 - INACCESSIBLE_BOOT_DEVICE
Error 0x0000002E - DATA_BUS_ERROR
Error 0x00000050 - PAGE_FAULT_IN_NONPAGED_AREA
The DRM attribute value is too small before disk scan

As this program is a scam do not be scared into purchasing the program when you see its alerts.



Overview

Hard Drive Health Status (A brief overview of reliability and performance of current hard drives)

Local Disk 1: C:\ (current status: Critical)

Disk model:
(Standard disk drives)
Capacity:
30 GB
Power-on time:
12 minutes

Reliability: 28% (critical) Performance: 34% (poor) Error resistance: 14% (critical)

Your disk is in a critical state. Click here for more S.M.A.R.T. details

Take required actions to prevent data loss.

Disk Monitoring Statistics

Relocated bad sectors: 2025
Pending bad sectors: 2440

Operating system: Windows XP Professional
Service pack: Service Pack 3 (Build 2600)
Processor: Intel(R) Core(TM) i7-2600K CPU @ 3.40GHz
RAM: 2 GB

SMART HDD Trial version. Click here to activate

Smart HDD screen shot
For more screen shots of this infection click on the image above.
There are a total of 3 images you can view.

If you are infected with Smart HDD it is important that you do not delete any files from your Temp folder or use any temp file cleaners. This is because when the infection is installed it will delete shortcuts found in various locations and store backups of them in the **%Temp%\smtmp** folder. It does this so that you when try to launch a program from your

Search Security Guides

Search

Share

5 364 Like 28 Tweet 1 Share

Latest Viruses

Windows Safety Wizard
Windows TurnKey Console
Windows Malware Firewall
Live Security Platinum
Windows Antivirus Rampart
Windows Ultimate Security Patch
Windows Defence Counsel
Windows Guard Tools
Windows Safety Maintenance
System Protection Tools
Windows Multi Control System
Windows Private Shield
Windows Pro Safety
Windows Pro Safety Release

Threat Descriptions

Adware
Ransomware
Rogue Programs & Scareware
Rootkits
Spyware
Trojan Horses
Worms

start menu, none of your shortcuts will appear and thus making you think that your computer has a serious problem. Therefore, you do not want to delete any of the files in your Temp folder as it will remove the backups that we will use later in the guide to restore your Windows Start Menu. For a list of folders that shortcuts are deleted and the corresponding directories where they are stored, please see this topic: **Unhide.exe - A introduction as to what this program does**.

To further make it seem like your computer is not operating correctly, System Check will also hide almost all of the files on your computer. This is done to make it seem like there is corruption on your hard drive that is causing your files to not be displayed. It does this by adding the **+H**, or hidden, attribute to all of your files, which causes your files to become hidden. It will then change your Windows settings so that you cannot view hidden and system files. Once the rogue's processes are terminated you can change a setting in Windows so that you can view hidden files and thus be able to see your files and folders again. Instructions on how to enable the viewing of hidden files can be found in the following tutorial:

> **How to see hidden files in Windows**

Smart HDD also attempts to make it so you cannot run any programs on your computer. If you attempt to launch a program it will terminate it and state that the program or hard drive is corrupted. It does this to protect itself from anti-virus programs you may attempt to run and to make your computer unusable so that you will be further tempted to purchase the rogue. The messages that you will see when you attempt run a program are:

> **Windows detected a hard drive problem.**
> A hard drive error occurred while starting the application.
>
> Or
>
> Windows cannot find notepad. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button, and then click Search.

These are just further alerts trying to make you think your computer has a serious hard drive problem. It should be noted that if you attempt to run a program enough times it will eventually work.

As you can see, this program was designed to make you think your hard drives are failing and that your data is lost. In reality, though, the hard drives are fine and your data has not been deleted. Therefore, do not purchase Smart HDD for any reason, and if you already have, please contact your credit card company and state that the program is a computer infection and a scam and that you would like to dispute the charge. To remove this infection and related malware, please follow the steps in the guide below.

Threat Classification:

- **Information on Rogue Programs & Scareware**

Advanced information:

> **View Smart HDD files.**
> **View Smart HDD Registry Information.**

Tools Needed for this fix:

- **Malwarebytes' Anti-Malware**

Symptoms that may be in a HijackThis Log:

```
O4 - HKCU\..\Run: [<random>] %Temp%\<random>.exe
O4 - HKCU\..\Run: [<random>.exe] %Temp%\<random>.exe
```

Guide Updates:

> *12/14/10 - Initial guide creation.*
> *04/01/12 - Updated for new variant.*

Automated Removal Instructions for Smart HDD using Malwarebytes' Anti-Malware:

1. Print out these instructions as we may need to close every window that is open later in the fix.
2. Reboot your computer into **Safe Mode with Networking**. To do this, turn your computer off and then back on and immediately when you see anything on the screen, start tapping the **F8** key on your keyboard. Eventually you will be brought to a menu similar to the one below:

Follow BleepingComputer.com

Archives

Forum Guides

Latest Forum Discussions

Task Manager won't come up.

.x

boot device priority changes every time...

Can't remove Sireref.AK

atraps.gen2 Avira warnings

Latest Tutorials

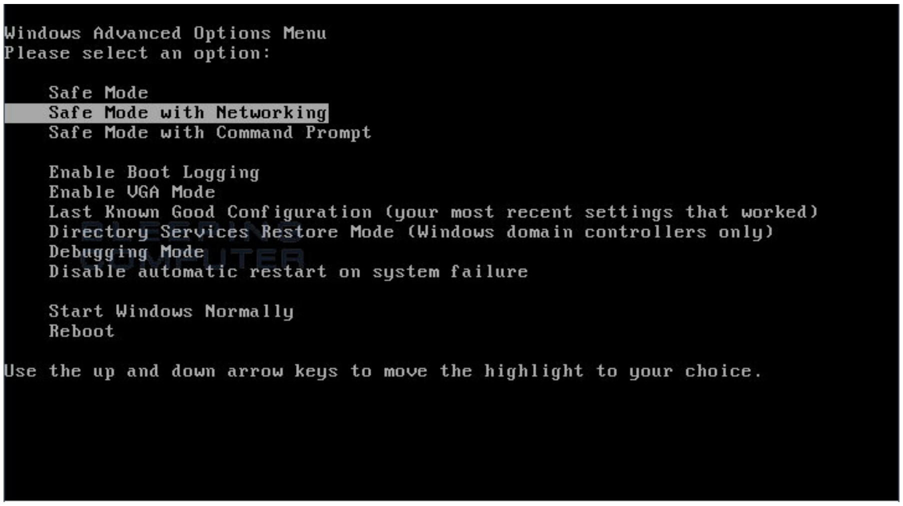
How to use the Windows Recycle Bin

How to disable silent and automatic updates in Chrome for Windows

How to disable Silent Updates in Firefox

An Introduction to your Computer

How to change or select which program starts when you double-click a file in Windows 8



```
Windows Advanced Options Menu
Please select an option:

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable VGA Mode
    Last Known Good Configuration (your most recent settings that worked)
    Directory Services Restore Mode (Windows domain controllers only)
    Debugging Mode
    Disable automatic restart on system failure

    Start Windows Normally
    Reboot

Use the up and down arrow keys to move the highlight to your choice.
```

Using the arrow keys on your keyboard, select **Safe Mode with Networking** and press **Enter** on your keyboard. If you are having trouble entering safe mode, then please use the following tutorial: **How to start Windows in Safe Mode**

Windows will now boot into safe mode with networking and prompt you to login as a user. Please login as the same user you were previously logged in with in the normal Windows mode. Then proceed with the rest of the steps.

3. It is possible that the infection you are trying to remove will not allow you to download files on the infected computer. If this is the case, then you will need to download the files requested in this guide on another computer and then transfer them to the infected computer. You can transfer the files via a CD/DVD, external drive, or USB flash drive.

4. Before we can do anything we must first end the processes that belong to Smart HDD so that it does not interfere with the cleaning procedure. To do this, please download RKill to your desktop from the following link.

   RKill Download Link - (Download page will open in a new tab or browser window.)

   When at the download page, click on the **Download Now** button labeled **iExplore.exe download link**. When you are prompted where to save it, please save it on your **desktop**.

5. Once it is downloaded, double-click on the **iExplore.exe** icon in order to automatically attempt to stop any processes associated with Smart HDD and other Rogue programs. If you cannot find the iExplore.exe icon that you downloaded, you can also execute the program by doing the following steps based on your version of Windows:

   For Windows 7 and Windows Vista, click on the **Start** button and then in the search field enter **%userprofile%\desktop\iexplore.exe** and then press the **Enter** key on your keyboard. If you Windows prompts you to allow it to run, please allow it to do so.

   For Windows XP, click on the **Start** button and then click on the **Run** menu option. In the **Open:** field enter **%userprofile%\desktop\iexplore.exe** and press the **OK** button. If you Windows prompts you to allow it to run, please allow it to do so.

   Please be patient while the program looks for various malware programs and ends them. When it has finished, the black window will automatically close and you can continue with the next step. If you get a message that RKill is an infection, do not be concerned. This message is just a fake warning given by Smart HDD when it terminates programs that may potentially remove it. If you run into these infections warnings that close RKill, a trick is to leave the warning on the screen and then run RKill again. By not closing the warning, this typically will allow you to bypass the malware trying to protect itself so that rkill can terminate Smart HDD . So, please try running RKill until the malware is no longer running. You will then be able to proceed with the rest of the guide. **If you continue having problems running RKill, you can download the other renamed versions of RKill from the rkill download page. All of the files are renamed copies of RKill, which you can try instead. Please note that the download page will open in a new browser window or tab.**

   Do not reboot your computer after running RKill as the malware programs will start again.

6. As this infection is known to be bundled with the TDSS rootkit infection, you should also run a program that can be used to scan for this infection. Please follow the steps in the following guide:

   How to remove Google Redirects or the TDSS, TDL3, or Alureon rootkit using TDSSKiller

   If after running TDSSKiller, you are still unable to update Malwarebytes' Anti-malware or continue to have Google search result redirects, then you should post a virus removal request using the steps in the following topic rather than continuing with this guide:

   Preparation Guide For Use Before Using Malware Removal Tools and Requesting Help Topic

7. Now you should download Malwarebytes' Anti-Malware, or MBAM, from the following location and save it to your desktop:

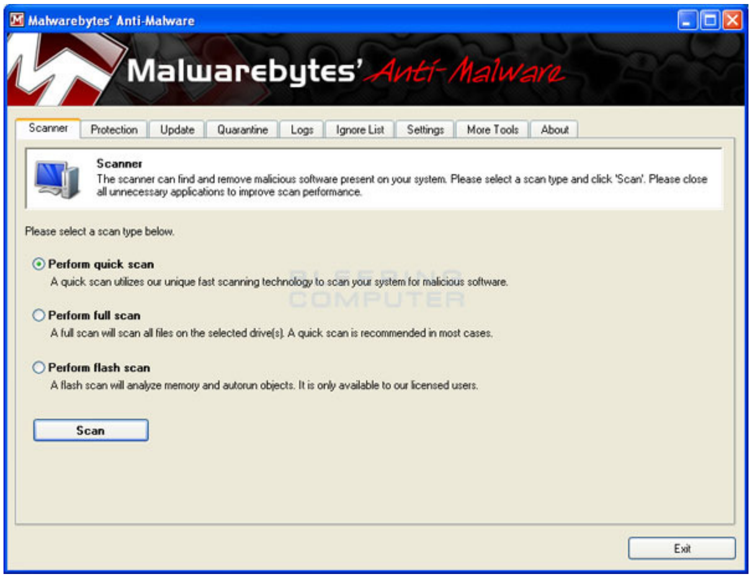
   Malwarebytes' Anti-Malware Download Link (Download page will open in a new window)

8. Once downloaded, close all programs and Windows on your computer, including this one.

9. Double-click on the icon on your desktop named **mbam-setup.exe**. This will start the installation of MBAM onto your computer.

10. When the installation begins, keep following the prompts in order to continue with the installation process. Do not make any changes to default settings and when the program has finished installing, make sure you leave both the **Update Malwarebytes' Anti-Malware** and **Launch Malwarebytes' Anti-Malware** checked. Then click on the **Finish** button. If MalwareBytes' prompts you to reboot, please do not do so.

11. MBAM will now automatically start and you will see a message stating that you should update the program before performing a scan. As MBAM will automatically update itself after the install, you can press the **OK** button to close that box and you will now be at the main program as shown below.



Scanner
The scanner can find and remove malicious software present on your system. Please select a scan type and click 'Scan'. Please close all unnecessary applications to improve scan performance.

Please select a scan type below.

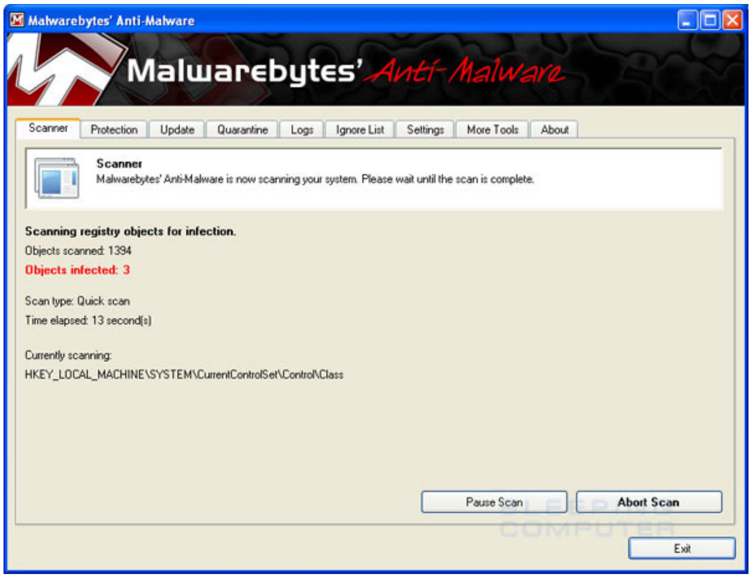
● Perform quick scan
A quick scan utilizes our unique fast scanning technology to scan your system for malicious software.

○ Perform full scan
A full scan will scan all files on the selected drive(s). A quick scan is recommended in most cases.

○ Perform flash scan
A flash scan will analyze memory and autorun objects. It is only available to our licensed users.

12. On the **Scanner** tab, make sure the the **Perform full scan** option is selected and then click on the **Scan** button to start scanning your computer for **Smart HDD** related files.

13. MBAM will now start scanning your computer for malware. This process can take quite a while, so we suggest you go and do something else and periodically check on the status of the scan. When MBAM is scanning it will look like the image below.



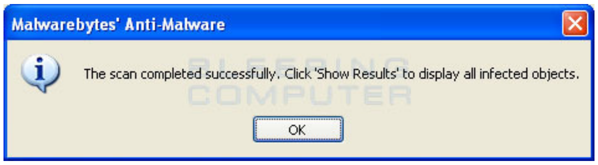
Scanner
Malwarebytes' Anti-Malware is now scanning your system. Please wait until the scan is complete.

Scanning registry objects for infection.
Objects scanned: 1394
Objects infected: 3

Scan type: Quick scan
Time elapsed: 13 second(s)

Currently scanning:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class

14. When the scan is finished a message box will appear as shown in the image below.

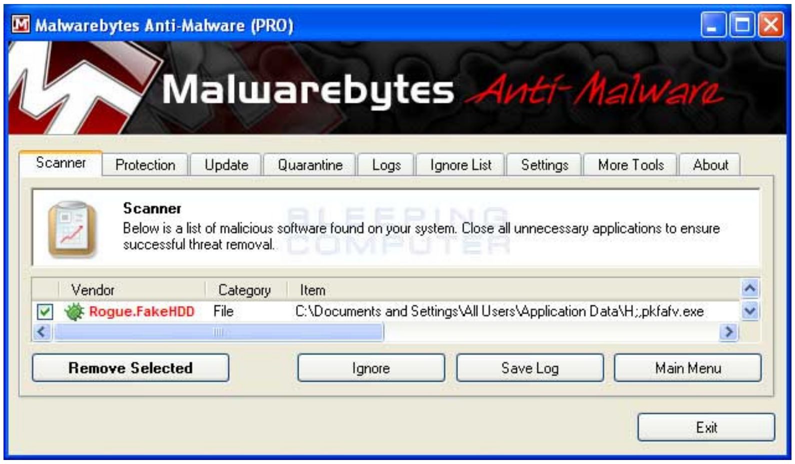


The scan completed successfully. Click 'Show Results' to display all infected objects.

You should click on the OK button to close the message box and continue with the **SmartHDD** removal process.

15. You will now be back at the main Scanner screen. At this point you should click on the **Show Results** button.

16. A screen displaying all the malware that the program found will be shown as seen in the image below. Please note that the infections found may be different than what is shown in the image.



Scanner

Below is a list of malicious software found on your system. Close all unnecessary applications to ensure successful threat removal.

	Vendor	Category	Item
☑	Rogue.FakeHDD	File	C:\Documents and Settings\All Users\Application Data\H;.pkfafv.exe

You should now click on the **Remove Selected** button to remove all the listed malware. MBAM will now delete all of the files and registry keys and add them to the programs quarantine. When removing the files, MBAM may require a reboot in order to remove some of them. If it displays a message stating that it needs to reboot, please allow it to do so. Once your computer has rebooted, and you are logged in, please continue with the rest of the steps.

17. When MBAM has finished removing the malware, it will open the scan log and display it in Notepad. Review the log as desired, and then close the Notepad window.

18. You can now exit the MBAM program.

19. This infection family will also hide all the files on your computer from being seen. To make your files visible again, please download the following program to your desktop:

    Unhide.exe

    Once the program has been downloaded, double-click on the Unhide.exe icon on your desktop and allow the program to run. This program will remove the +H, or hidden, attribute from all the files on your hard drives. If there are any files that were purposely hidden by you, you will need to hide them again after this tool is run.

20. As this infection changes your desktop background to a solid black color, we now want to change it back to the default Windows theme or to modify it to your preferences. If you are using Windows XP, please click on the **Start** button and then select **Control Panel**. When the Control Panel opens, please click on the **Display** icon. From this screen you can now change your Theme and desktop background so that it no longer shows the black background.

    If you are using Windows Vista or Windows 7, please click on the **Start** button and then select **Control Panel**. When the Control Panel opens, please click on the **Appearance and Personalization** category. Then select **Change the Theme** or **Change Desktop Background** to revert back to your original Theme and colors.

21. This rogue will also disable various menu items from appearing on the Windows Start Menu. To add these items back, please right-click on the Start button and select **Properties.** The start button for Windows XP looks like start and the Windows Vista and Windows 7 start button looks like . You will now be at the Taskbar and Start Menu Properties screen. Select the **Start Menu** tab and then click on the **Customize** button. If in Windows XP, you will now need to click on the **Advanced** tab. You will now be presented with a variety of menus and shortcuts that can be added back to the Windows Start Menu. Please select the various items you would like to add and then click on the **OK** button. Then press the **Apply** button and close the Start Menu properties screen.

22. You can now reboot your computer out of Safe Mode and back into your normal Windows Mode. When Windows has started and your back at your normal desktop, please continue with step 22.

23. Finally, as many rogues and other malware are installed through vulnerabilities found in out-dated and insecure programs, it is strongly suggested that you use Secunia PSI to scan for vulnerable programs on your computer. A tutorial on how to use Secunia PSI to scan for vulnerable programs can be found here:

    How to detect vulnerable and out-dated programs using Secunia Personal Software Inspector

Your computer should now be free of the **SmartHDD** program. If your current anti-virus solution let this infection through, you may want to consider **purchasing the PRO version of Malwarebytes' Anti-Malware** to protect against these types of threats in the future.

If you are still having problems with your computer after completing these instructions, then please follow the steps outlined in the topic linked below:

Preparation Guide For Use Before Using Malware Removal Tools and Requesting Help

Associated Smart HDD Files:

%AppData%\Microsoft\Internet Explorer\Quick Launch\SMART_HDD.lnk
%CommonAppData%\<random>
%CommonAppData%\-<random>
%CommonAppData%\<random>.exe
%CommonAppData%\-<random>r
%Desktop%\SMART_HDD.lnk
%StartMenu%\Programs\SMART HDD\
%StartMenu%\Programs\SMART HDD\SMART HDD.lnk
%StartMenu%\Programs\SMART HDD\Uninstall SMART HDD.lnk

File Location Notes:

%Desktop% means that the file is located directly on your desktop. This is C:\DOCUMENTS AND SETTINGS\<Current User>\Desktop\ for Windows 2000/XP, and C:\Users\<Current User>\Desktop\ for Windows Vista and Windows 7.

%CommonAppData% refers to the **Application Data** folder for the All Users Profile. By default, this is C:\Documents and Settings\All Users\Application Data for Windows 2000/XP and C:\ProgramData\ for Windows Vista/7.

%AppData% refers to the current users Application Data folder. By default, this is C:\Documents and Settings\<Current User>\Application Data for Windows 2000/XP. For Windows Vista and Windows 7 it is C:\Users\<Current User>\AppData\Roaming.

%StartMenu% refers to the Windows Start Menu. For Windows 95/98/ME it refers to C:\windows\start menu\, for Windows XP, Vista, NT, 2000 and 2003 it refers to C:\Documents and Settings\<Current User>\Start Menu\, and for Windows Vista/7 it is C:\Users\<Current User>\AppData\Roaming\Microsoft\Windows\Start Menu.

%CommonAppData% refers to the Application Data folder in the All Users profile. For Windows XP, Vista, NT, 2000 and 2003 it refers to C:\Documents and Settings\All Users\Application Data\, and for Windows Vista/7 it is C:\ProgramData.

Associated Smart HDD Windows Registry Information:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "<random>"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "<random>.exe"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings "CertificateRevocation" = 0
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings "WarnonBadCertRecving" = 0
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main "Use FormSuggest" = "Yes"
```

This is a self-help guide. Use at your own risk.

BleepingComputer.com can not be held responsible for problems that may occur by using this information. If you would like help with any of these fixes, you can ask for malware removal assistance in our Virus, Trojan, Spyware, and Malware Removal Logs forum.

If you have any questions about this self-help guide then please post those questions in our AntiVirus, Firewall and Privacy Products and Protection Methods forum and someone will help you.