Manual removal of GhostDNS details

You accidentally infected with GhostDNS and don't know what to do, because all the antivirus tools you use don't seem to eliminate this trojan successfully? This article will help you.

You accidentally infected with GhostDNS and don't know what to do, because all the antivirus tools you use don't seem to eliminate this trojan successfully? This article will help you. Let's find out soon!

Manual removal of GhostDNS details

What is GhostDNS?

GhostDNS is a dangerous trojan that can infiltrate the system without users knowing. It primarily attacks different versions of Windows computers and is capable of exploiting vulnerabilities. In the first phase, GhostDNS will make changes to the default security settings, desktop wallpaper, DNS configuration, DLL files, etc. of the system and users seem to not realize it. Its presence will slow down the performance of all basic functions on the system including startup, shutdown, file opening, game play, application installation, Internet connection, etc. It also will create unwanted icons, files or folders in different locations on the system. You will also detect changes in the content or extensions of the stored files. Therefore, if you detect any signs of GhostDNS, don't hesitate for a moment. Please remove it permanently immediately.

GhostDNS causes trouble for the system and turns it into a botnet. Usually it comes from the system directory by creating hidden files, making it difficult to detect malware as usual. Even more dangerous it can affect firewall and antivirus features. Moreover, it can observe sensitive information such as system login details, computer location and other information with the help of keyloggers. If somehow your PC is encountering this threat, you should act immediately to remove GhostDNS. In case you don't know what to do, read the steps below to remove this dangerous trojan.

How do you remove GhostDNS automatically?

A powerful tool that can detect, remove and block spyware (spyware), adware (adware), keyloggers, cookies, rootkits, trojans, worms and other types of malware. You can follow the antivirus removal guide below to remove the threat.

1. Download any powerful tool.

2. Perform a full scan or quick scan on your computer, after you have installed the selected antivirus tool.

3. Select the malicious files detected after scanning.

4. Click the **"Fix Threats"** button to remove all threats.

Some consequences caused by trojan virus

Trojan horses allow cybercriminals to infiltrate infected computers without being noticed and can disable executable programs installed on users' computers, causing system crashes. In addition, it will change important settings on your computer to allow cyber criminals to remotely control. In addition, it will modify registry settings and key key values, making this trojan very difficult to remove.

Things to remember

An effective tool can help you avoid unnecessary conflicts, mistakes and losses. You can remove all threats and troubleshoot from malware with just a few clicks. Try the simple step above to fix the problem with malware with an automated tool.

How to remove GhostDNS completely?

Most users find it difficult to remove GhostDNS from their computer. This is because GhostDNS is designed with the latest programming language and technology. Due to its changing properties, GhostDNS can easily get rid of being detected and removed by regular antivirus programs. There are 3 methods to remove GhostDNS as follows:

1. Method 1: Remove trojan horse using SpyHunter.
2. Method 2: Remove trojan horse by using StopZilla.
3. Method 3: Remove each step of Trojan horse manually.

Method 1: Remove trojan horse using SpyHunter.

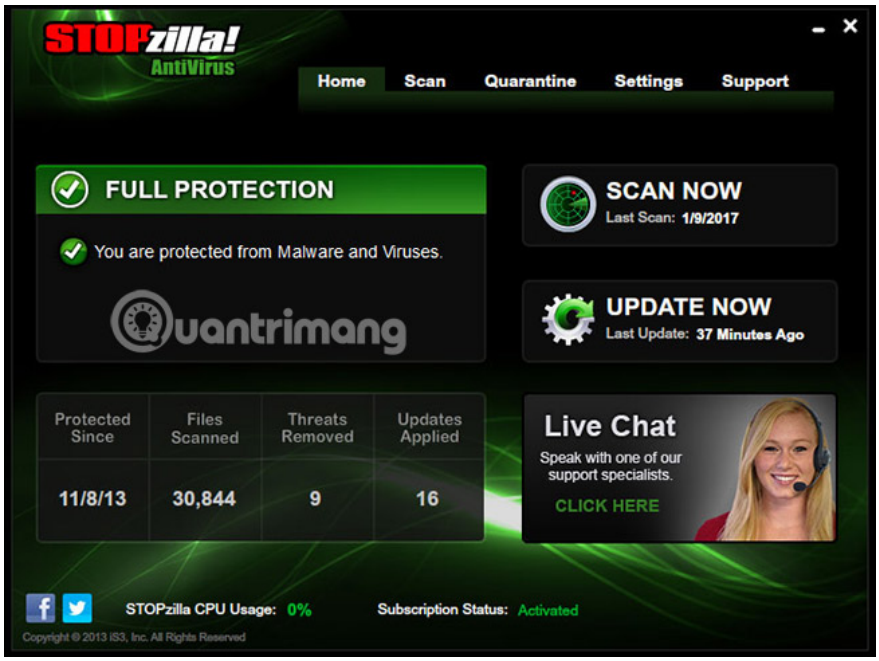
SpyHunter is an excellent malware removal tool that eliminates many different types of malware such as trojans, worms, adware, viruses, rootkits, spyware, ransomware, etc. Now you can download and use it. This powerful tool to remove GhostDNS from your computer. Please download Spyhunter and follow the steps in the article: How to use SpyHunter to remove spyware and anti-keyloggers to do this.

Method 2: Remove trojan horse by using StopZilla.

AVM technology provides the most flexible protection against online threats. Using dual engine technology, STOPzilla AntiVirus configures itself into **Full Protection Mode** or **Shared Protection Mode** . It combines with other security solutions to protect your system against viruses in the best way.

1) Download STOPzilla.

2) Click the **"Scan Now"** button to scan in full or quickly scan your PC after installing STOPzilla.

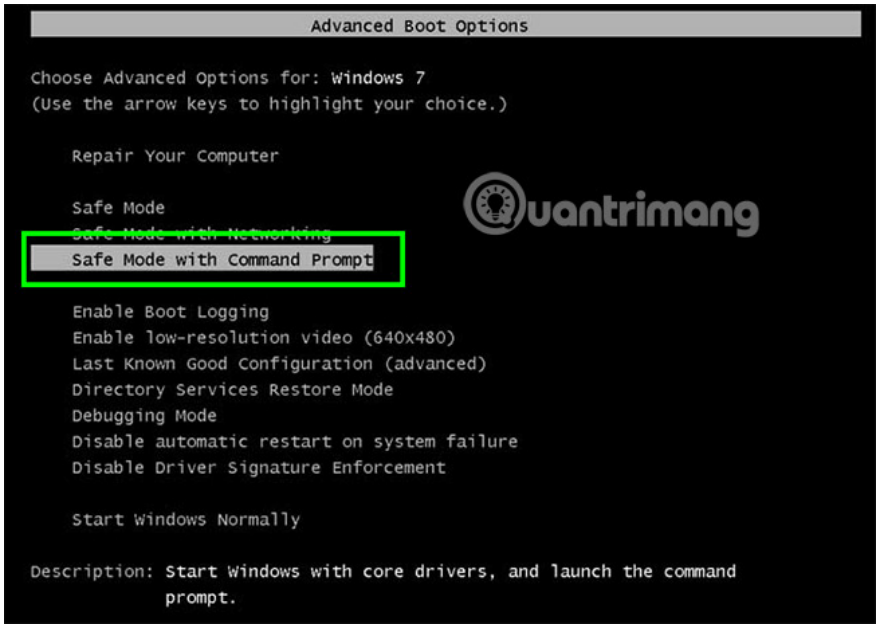


3) Select malicious files detected after scanning.

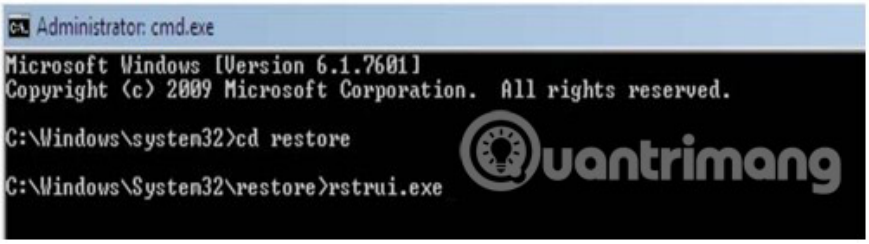
4) Click the **"Purge"** button on the right to delete all threats.

Method 3: Restore the system in Safe Mode with Command Prompt

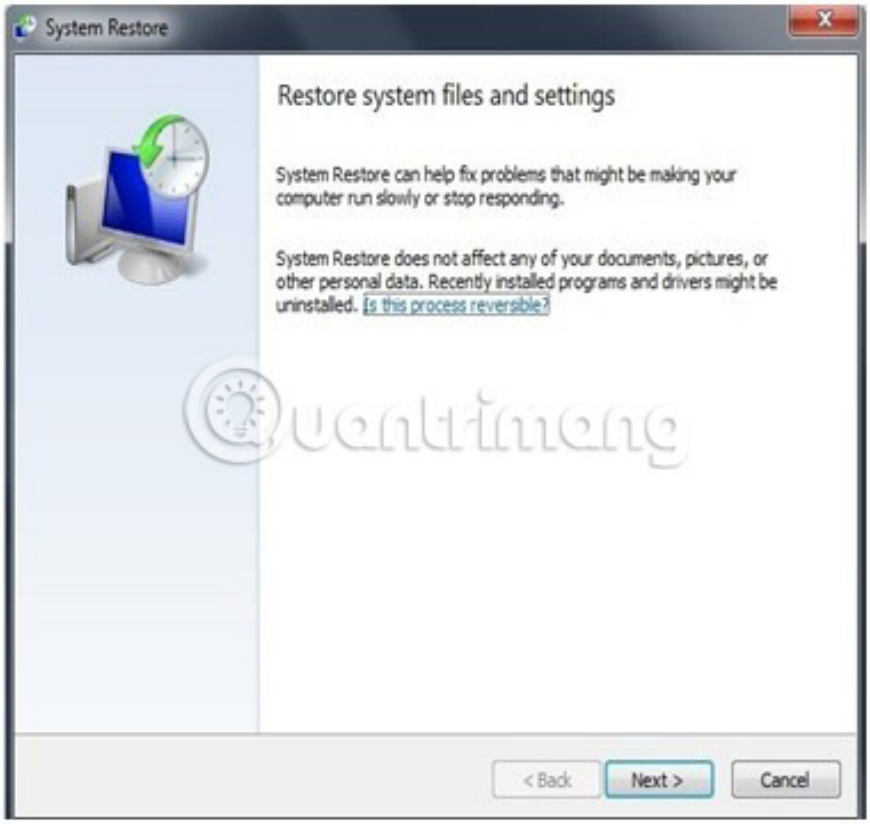
Step 1 : Restart your computer. When you see something appear on the screen, press the **F8** key and this step will bring you to the advanced boot options. Select the option ' **Safe Mode with Command Prompt** ' and press **Enter.**

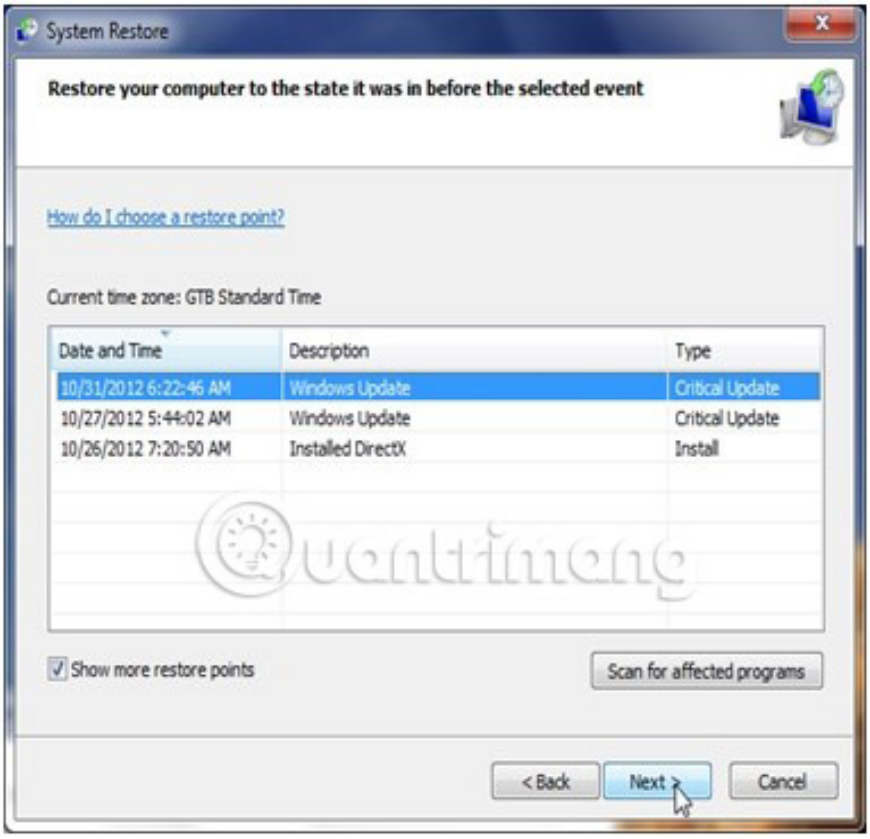


Step 2 : First, type **'restore cd'** and press **Enter.** Then type **'rstrui.exe'** and press **Enter** again.

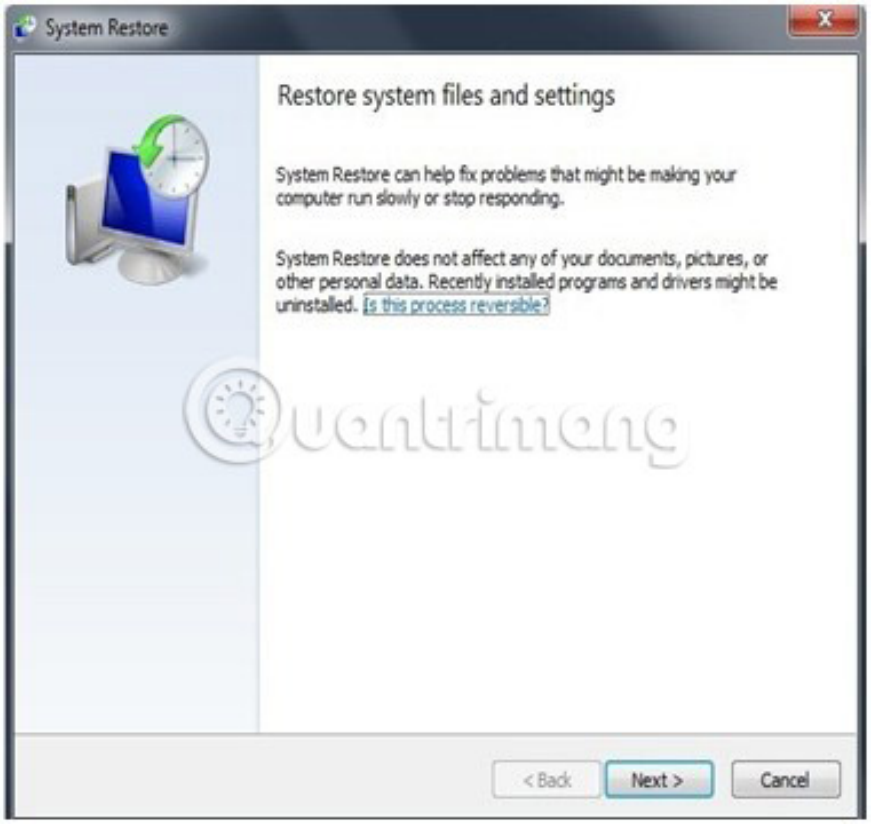


Step 3 : When the **System Restore** window appears, click **Next.** Select the restore point before your Trojan horse is infected and click **Next.**





Step 4 : Click **Yes** to continue. After that, the system restore task will start. After the system is restored, restart your computer to normal mode. Check if GhostDNS has been completely deleted from your computer.



Tips to keep your PC safe

1. Make sure you update your operating system and antivirus program on a regular basis.
2. Never download free software or pirated software from untrusted sites.
3. Take precautions when receiving strange emails from unknown people. Do not open the attachment or click the link contained in the letter.
4. Read the terms and agreements before installing a software on your computer. Uncheck the suspicious option toolbars or programs.
5. Avoid clicking attractive links or pop-up ads on strange websites.
6. Always scan your removable storage media for malware before opening them.

Wish you successfully removed GhostDNS!

See more:

1. 7 computer viruses you should be careful
2. Distinguish malware, viruses and Trojan horses
3. Warning 5 new viruses are quickly infected on the network

You finished reading the article "**Manual removal of GhostDNS details**" 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.