Instructions for removing DNS Unlocker adware

DNS Unlocker is a software that displays coupons at sites you visit or will compare prices when you are viewing a product on a site like Amazon. Although it sounds useful, the DNS Unlocker will invade and display ads whether you want it or not.

DNS Unlocker is a software that displays coupons at sites you visit or will compare prices when you are viewing a product on a site like Amazon. Although it sounds useful, the DNS Unlocker will invade and display ads whether you want it or not.

Once you have installed this utility, it will display banner ads, pop up or run text with information such as **"Powered by DNS Unlocker", "Brought to you by DNS Unlocker", "You've received a premium offer from DNS Unlocker "** . These ads aim to "lure" users to install additional tools, extensions and owners of DNS Unlocker that will benefit from users' clicks.

When "Unlocking" DNS Unlocker, your device will have a number of expressions:

1. Banner ads will be included in the websites you visit
2. Text on random webite will turn into links
3. Pop up ads on the browser will introduce you to fake updates or other software.
4. Other unwanted adware will automatically install.

1. How does DNS Unlocker get into your computer?

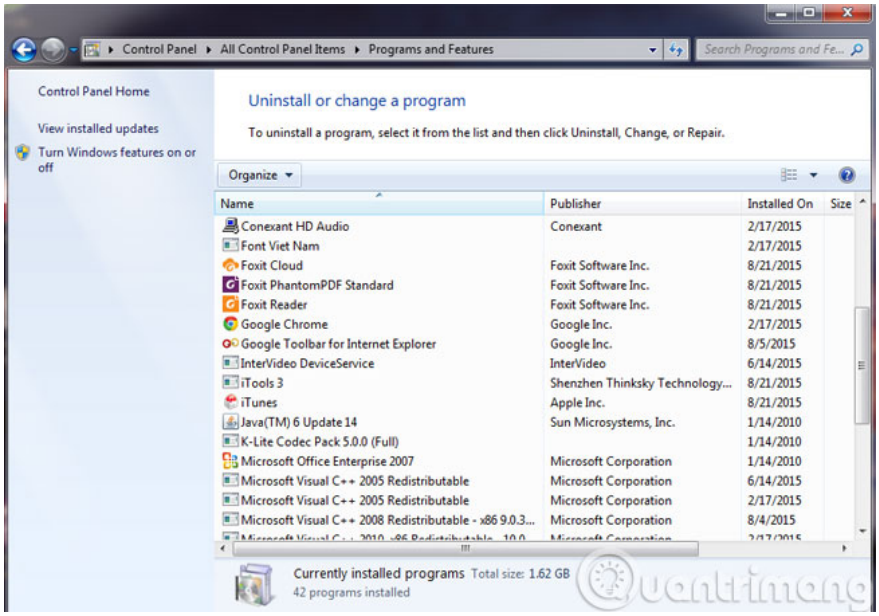
DNS Unlocker usually comes with other free software that you download from the Internet. You should be careful when installing a software because it has very good settings such as DNS Unlocker.

2. How to remove DNS Unlocker

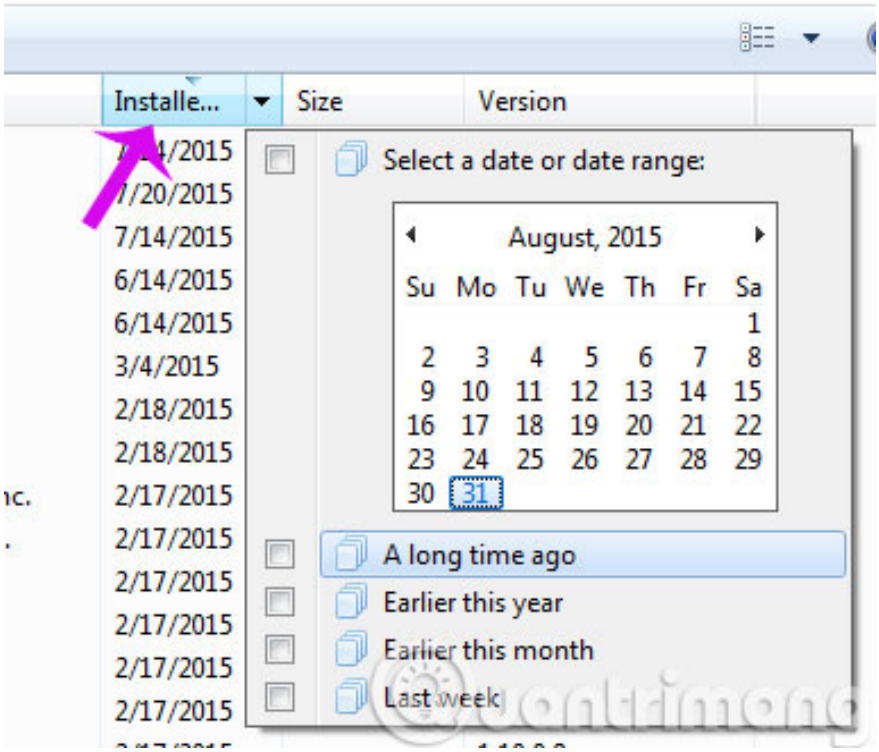
Step 1:

Uninstall DNS Unlocker from Windows

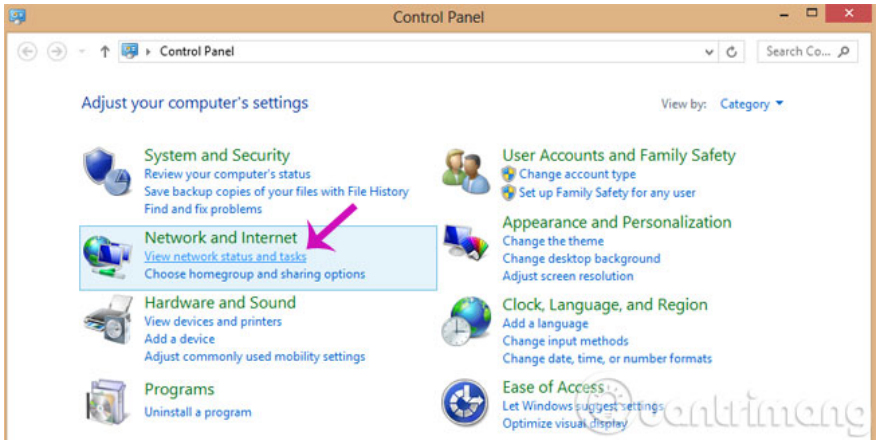
You access **Control Panel** , select **Program and Feature**

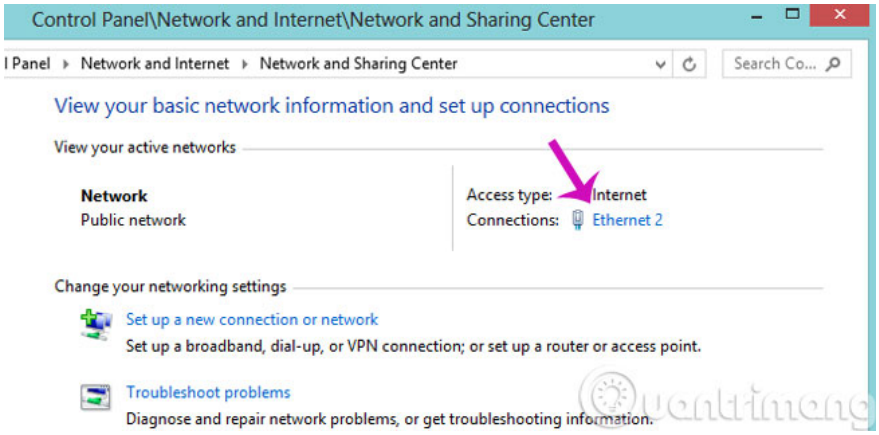


Here, you find software called **DNS Unlocker** and then click **Uninstall** . Malware may have a different name on your computer, to see recently installed software, you can click the **Installed On** column to sort by date. You search the list and remove any software that you don't know or don't use.

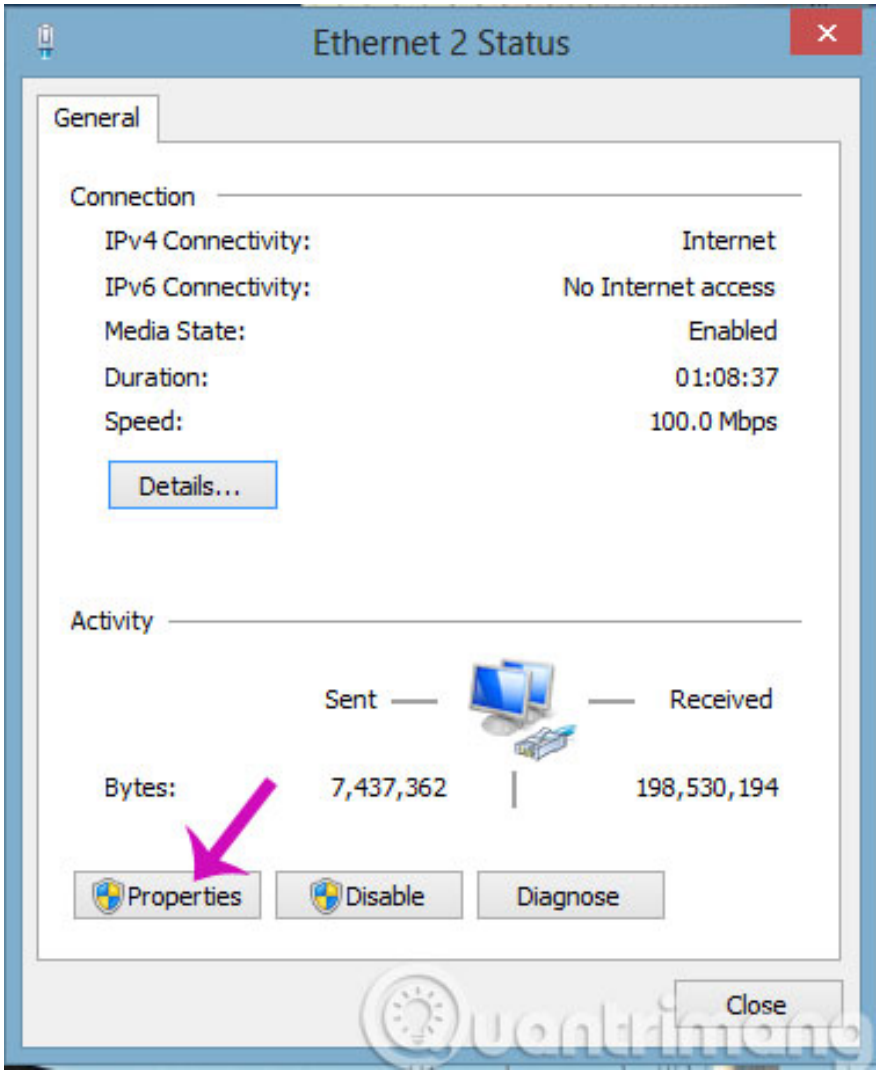


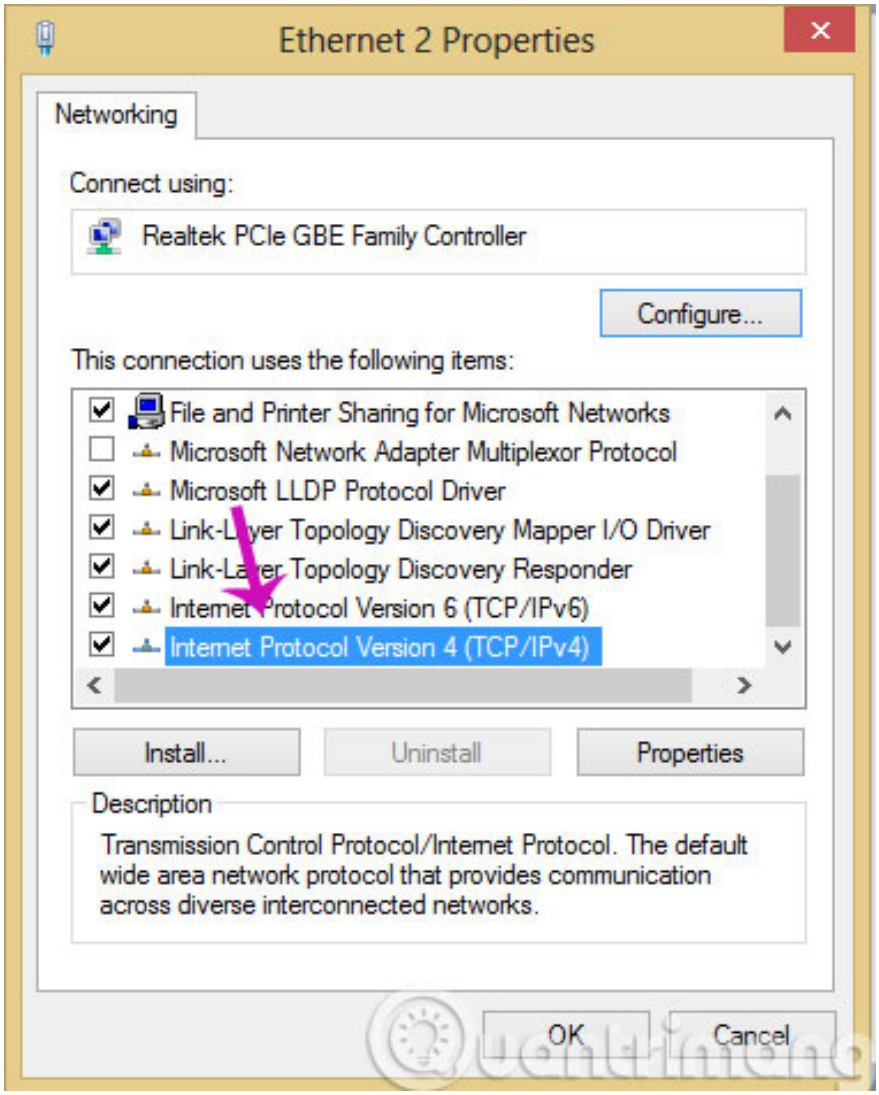
Next, still in the Control Panel, open View network status and tasks, click Ethernet 2



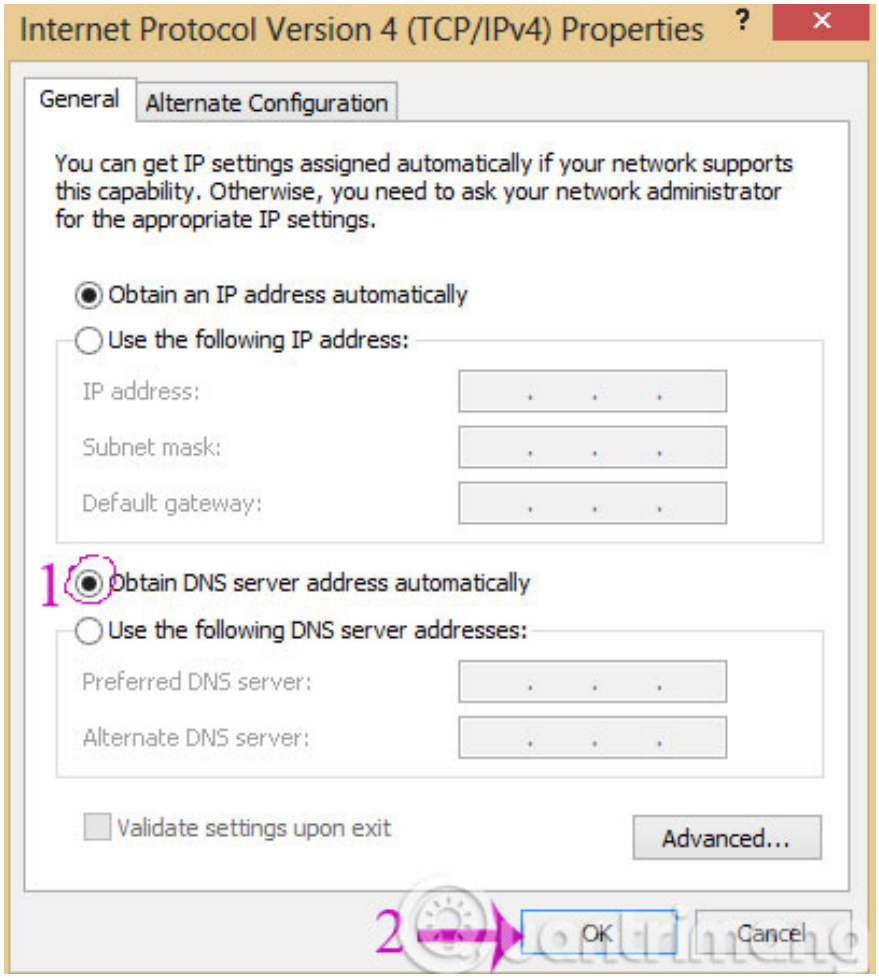


In the dialog box that opens, click Properties> Internet Protocol version 4


Ethernet 2 Status
General
Connection
IPv4 Connectivity:
Internet
IPv6 Connectivity:
No Internet access
Media State:
Enabled
Duration:
01:08:37
Speed:
100.0 Mbps
Details...
Activity
Sent
Received
Bytes:
7,437,362
198,530,194
Properties
Disable
Diagnose
Close



Next, check the Obtain DNS Server address box automatically and click OK



If you still don't find any "suspicious" software, go to the next step.

Step 2:

Remove DNS Unlocker with **AdwCleaner** software

Before opening AdwCleaner, close all other programs and web browsers. When you open AdwCleaner, click **Scan** as shown below.

AdwCleaner will start searching for DNS Unlocker files installed on your computer. To remove these DNS Unlocker files, click **Cleaning** .

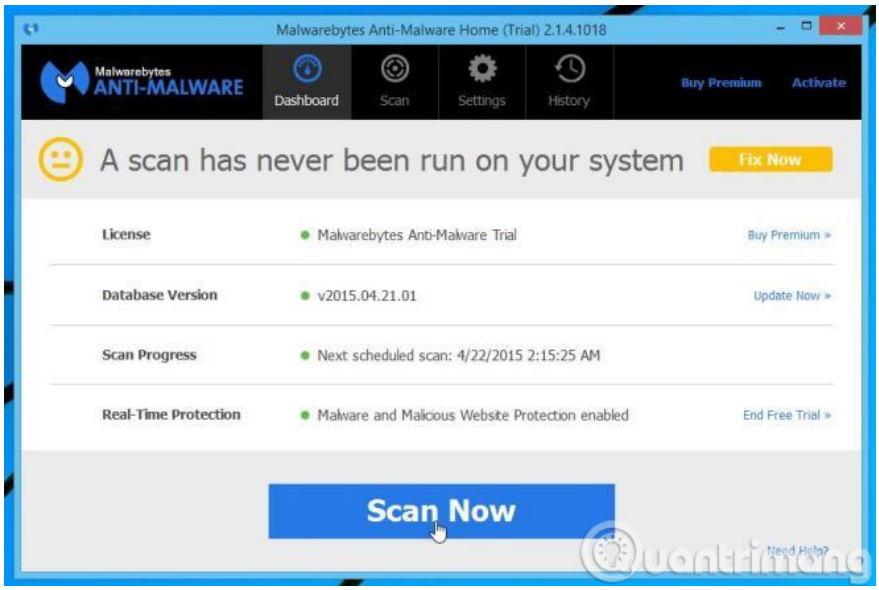
Then, click **OK** when the program requires to save the file, the file is open before restarting the computer.

Step 3:

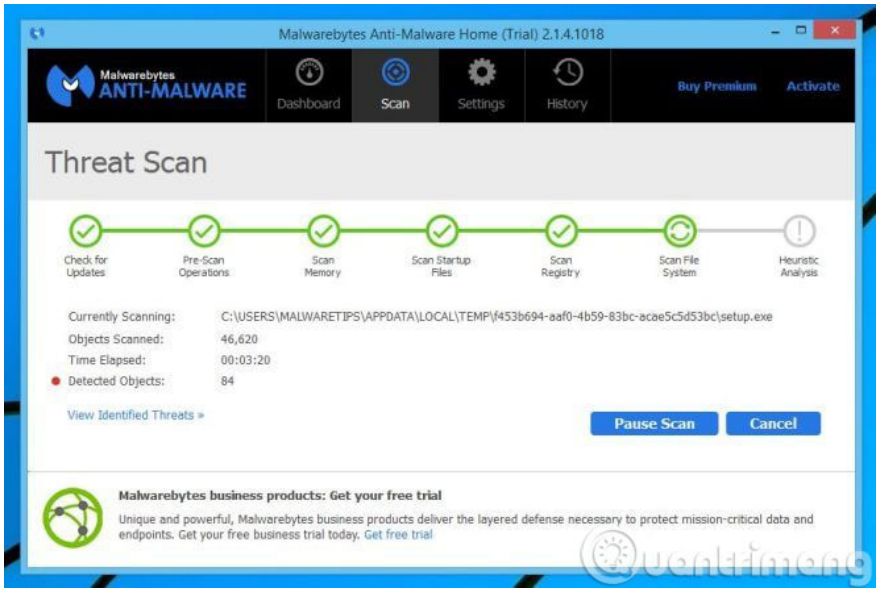
Remove DNS Unlocker with **Malwarebytes Anti-Malware**

Malwarebytes Anti-Malware uses the leading technology to detect and destroy malware including worms, Trojans, Spyware . It is important to note that it works well and should run in parallel with the software. Kill the virus without worrying about conflicts.

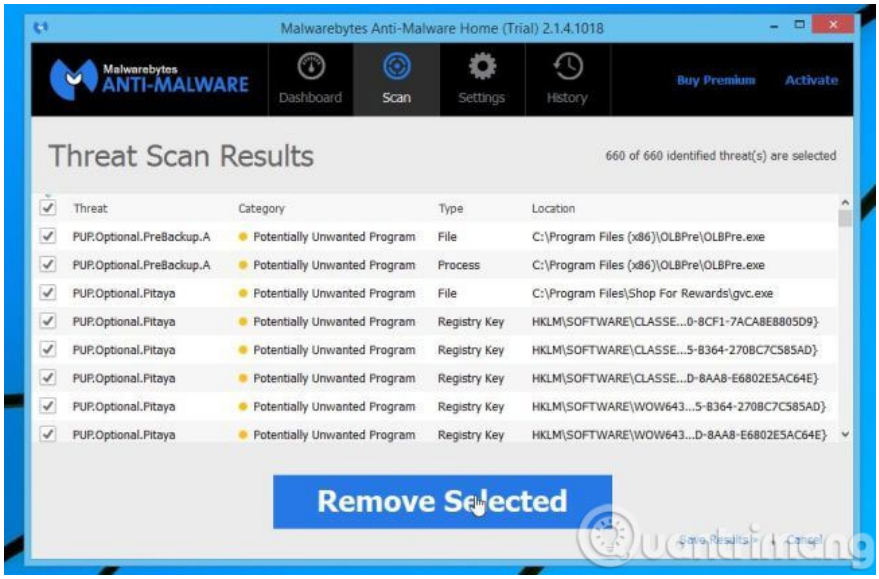
After successful installation, to scan the system, please click **Scan Now** .



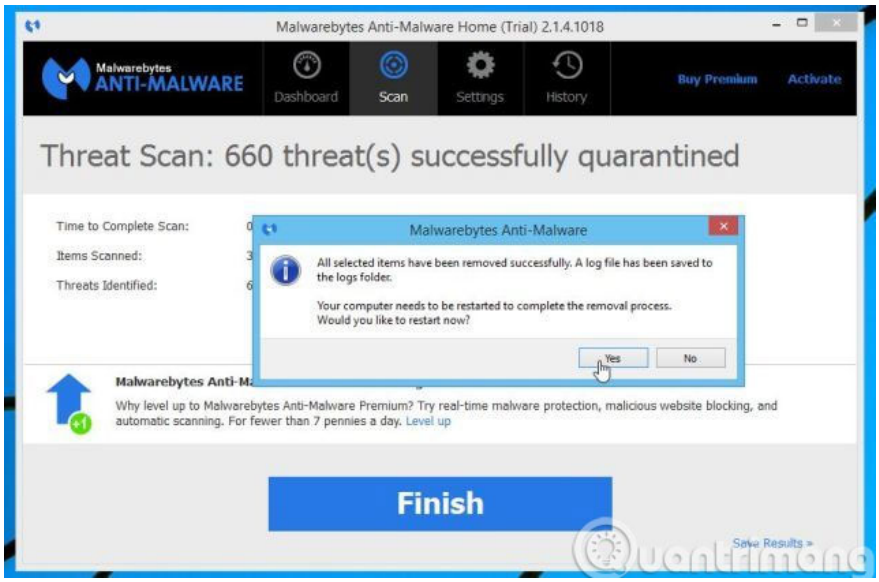
Malwarebytes Anti-Malware will start scanning computers to find DNS Unlocker.



After the scan is complete, the list of malware will be displayed on the screen. To remove them, click **Remove Selected** .



Malwarebytes will isolate malicious files and lock them. When removing those files, Malware will require a reboot. Please click **Yes** to restart the computer.



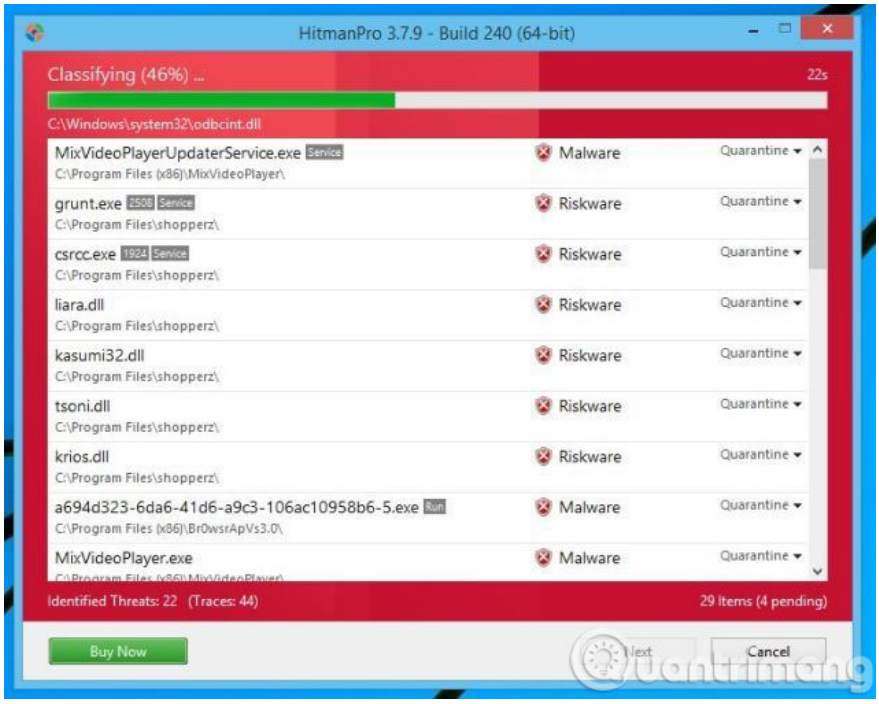
After restarting, you should scan again to make sure that the DNS Unlocker has been completely removed.

Step 4:

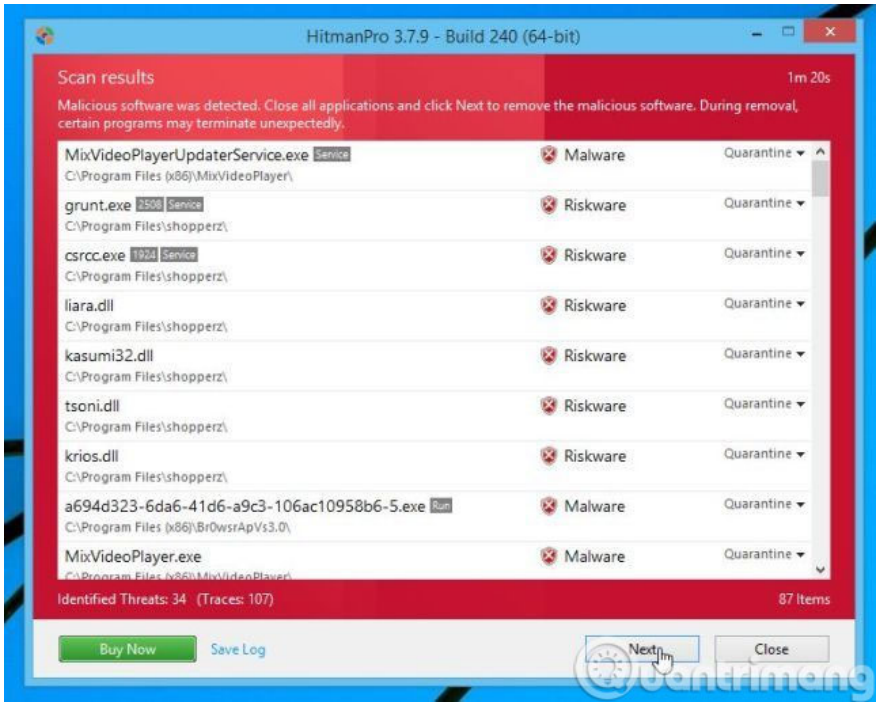
Check 2 times DNS Unlocker with **Hitmanpro**

Hitmanpro is the second protection measure to save infected computers Malware (virus, Trojan .) even though you have taken all security measures. Hitmanpro is designed to work with existing security programs without conflict. It scans quickly (less than 5 minutes) and doesn't slow down your computer.

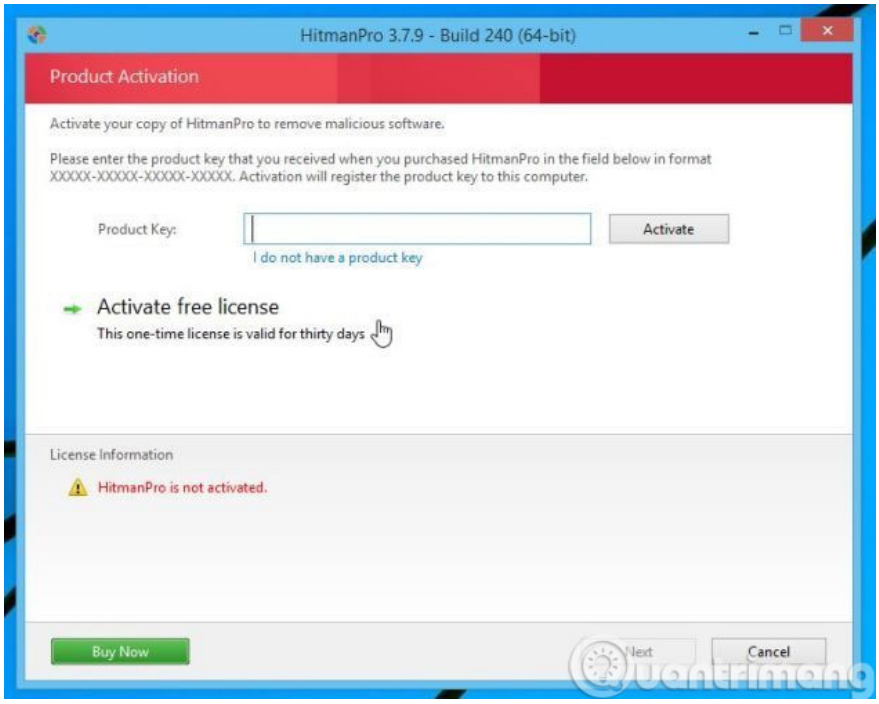
After successful installation, Hitmanpro will start scanning to find DNS Unlocker



When the scan is complete, the list of detected malware will be displayed, click **Next** to remove them



Next, click **Active free license** to try it for 30 days and remove the malware in the computer.

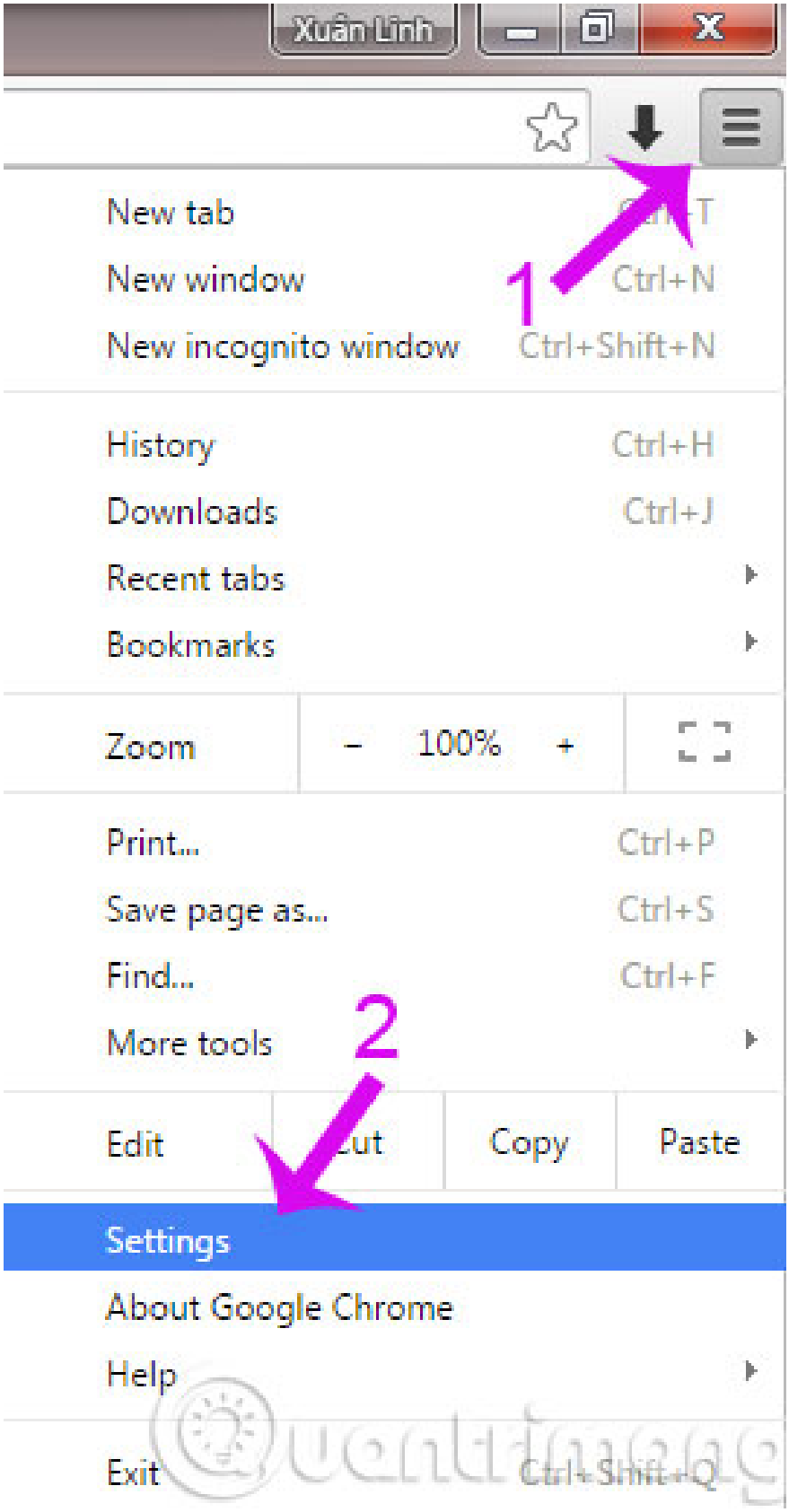


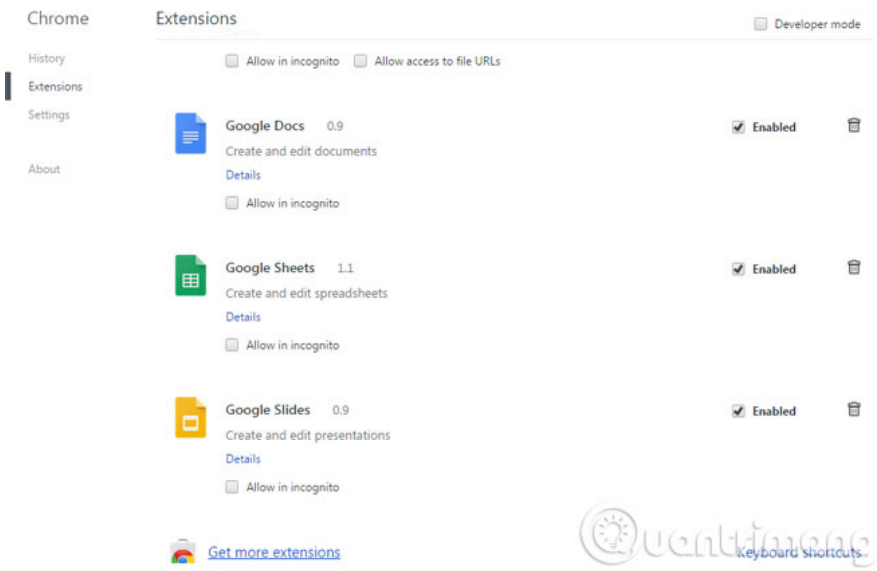
Step 5:

Reset **Chrome** and **Firefox settings** to remove DNS Unlocker

If you still have problems with DNS Unlocker, reset your browser to default.

At Google Chrome interface, click **Settings** , select **Extensions** tab. In the **Extensions** tab, delete DNS Unlocker or any extension you don't know about.


Xuân Linh
New tab
New window Ctrl+N
New incognito window Ctrl+Shift+N
History Ctrl+H
Downloads Ctrl+J
Recent tabs
Bookmarks
Zoom − 100% +
Print... Ctrl+P
Save page as... Ctrl+S
Find... Ctrl+F
More tools
Edit Cut Copy Paste
Settings
About Google Chrome
Help
Exit Ctrl+Shift+Q
1
2



Above are all steps to completely remove DNS Unlocker malware that we send you.

1. Risks from malware and how to prevent it
2. How to block ads when surfing the web
3. Some simple tricks to deal with Malware

Good luck!

You finished reading the article "**Instructions for removing DNS Unlocker adware**" 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.
