Did the fake DNSChanger change your DNS settings?

Domain Name System or DNS system is an Internet service that converts domain names into Internet protocol (IP) numbers. These digital IP addresses are used by computers to connect with each other.

Domain Name System or DNS system is an Internet service that converts domain names into Internet protocol (IP) numbers. These digital IP addresses are used by computers to connect with each other.

When you enter the domain name into the browser address bar, your computer will contact the DNS server. After that, it will find the IP address for that site. When this is done, your computer will use this IP address to connect to the site.

DNSChanger

The German Federal Information Security Office recently advised computer users to check DNS server settings on their computers or if the home network has been hacked. This responds to the success of the FBI in removing botnets. Ghost-Klick DNSChanger botnet has infected about 4 million computers in more than 100 countries. The Trojan redirected the requests of infected computers to malicious websites, by changing the address of the DNS server (reported by blog.eset.com).

For example, in this case, you can enter **https://quantrimang.com** and want to access this site, but you may suddenly find yourself accessing some other websites instead! This is due to fraud and DNS cache poisoning.

Although all malicious DNS servers have been replaced by the correct operating system during the uninstallation process, this may be the right time to see if your PC is really compromised.

To do so you can access **grc.com** . On this site, you can check if your home network or computer's DNS settings have been changed or controlled. Here, you can also check if your computer is compromised by this malware

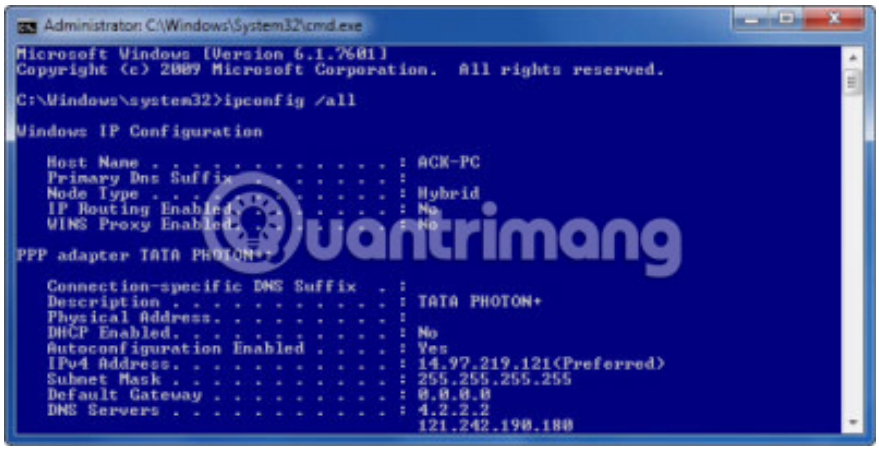
and change the DNS settings on your computer or home network. If you believe you have become a victim of DNSChanger, you can also check and report your IP to the FBI at **https://forms.fbi.gov/check-to-see-if-your-computer- is-using-rogue-DNS # googtrans (vi)** .

Botnets have changed the DNS settings of computer users and led them to malicious websites. Malicious DNS servers will provide fake, harmful, altering user searches and advertising fake and dangerous products. Because all web searches start with DNS, malware will show users of the changed Internet version. This form of fraud helped hackers steal over $ 14 million (according to the FBI).

How to find out if your computer is infected with DNSChanger

If you want to find out if your DNS settings have been compromised, you can do the following:

Open **CMD** and in the command window, type **ipconfig / all** and press **Enter.**



Now look for items starting with ' **DNS Servers .** '. It displays the IP address for your DNS servers in the format ddd.ddd.ddd.ddd, where ddd is a digit between 0 and 225. Record the IP address for the DNS server. Test them based on the numbers mentioned in the table that contain the known fake IP addresses. If you see a match, your computer is using fake DNS.

Rogue DNS Servers

85.255.112.0 through 85.255.127.255	To make the comparison between the computer's DNS servers and this table easier, start by comparing the first number before the first dot. For example, if your DNS servers do not start with 85, 67, 93, 77, 213, or 64, you can move on to the next step. If your servers start with any of those numbers, continue the comparison.
67.210.0.0 through 67.210.15.255	
93.188.160.0 through 93.188.167.255	
77.67.83.0 through 77.67.83.255	
213.109.64.0 through 213.109.79.255	
64.28.176.0 through 64.28.191.255	

If your computer is configured to use one or more fake DNS servers, it may have been infected with DNSChanger malware. Then, you should back up your files and scan your entire Windows computer with your antivirus software.

DNSChanger removal tool

You can use the DNSChanger Removal tool to fix this problem. If you need more help, you can contact us at any time.

See more:

1. Introducing DNS Resolver 1.1.1.1
2. What is DNS and DNS Lookup?
3. The new DNS service Quad9 helps block malicious domains

You finished reading the article "**Did the fake DNSChanger change your DNS settings?**" 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.
