Learn about DNS Hijacking and how to prevent it!

DNS Hijacking is a form of redirecting website addresses that users access. Understandably, you type the address abc.com into your browser, but you are actually being directed to another address, for example xyz.com.

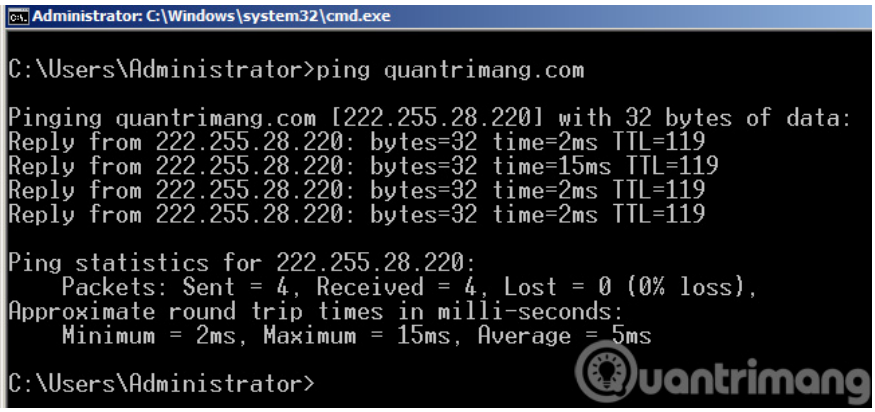
In technology, the term DNS - short for **Domain Name Resolution** is used to refer to address resolution, or in short, to solve the problem, to navigate the URL when you enter the address into the Address bar on the browser. . Easier to understand, DNS makes it easy and quick to access the IP address of the website you want to visit.

Besides, DNS Cache - or DNS caching, refers to DNS information on the local computer, which contains the resolved IP address of the websites you visit frequently (similar to Browser cookies like that). The idea of ?? DNS Cache is to help users save time when accessing websites regularly, but this is a good bait for hackers when the DNS Cache contains personal information of users. And the most common hacker job in this case is to attack, take ownership of DNS Cache, change the user's IP address to another fake website address.

1. What is DNS Hijacking?

DNS Hijacking is a form of redirecting website addresses that users access. Understandably, you type **abc.com** into your browser, but in fact you are "being" navigated to another address, for example **xyz.com** .

You can see that most domains - Domains of web pages are placed as text (eg, **quantrimang.com**), with each URL having an IP address corresponding to that URL, and the task The main part of DNS is to resolve, convert text characters (**quantrimang.com**) into the corresponding IP (you open **RUN** command> type " **ping** " to the domain that will output the IP address of that website). Specific examples:



What is the most common way of hackers in this case? They will entice users to install a certain piece of malware on the computer, usually Malware, and this malware will have the main task of changing the DNS of the computer system. Every time a user enters the address of any website, the system will automatically connect to the hacker's fake DNS server (instead of the DNS actually used by **ICANN - The Internet Corporation for**

Assigned Names and Numbers) and Navigate users to fake hacker websites.

See more:

1. What is PROXY?
2. What is SOCKS?

2. DNS Hijacking and DNS Cache Poisoning:

Both of these attack methods happen locally - that is, the user's computer. They are assigned very specifically:

1. **DNS Hijacking** : the task of installing malware on a user's computer.
2. **DNS Cache Poisoning** (or also called **Spoofing**): hijack DNS Cache and change the value and information in it to fake information.

For example, when you type the **quantrimang.com** address into the address bar of the browser, the system will confirm the IP address information corresponding to the domain name quantrimang.com and return the information to the computer (the result is the quantrimang.com website fully displayed on the browser). A domain name may contain multiple IP addresses, and when you visit quantrimang.com regularly, the system will recognize this as a website to remember, to shorten the time for subsequent visits.

Besides, this difference is exploited by hackers quite thoroughly (of course they have prepared many fake DNS servers), and among many fake DNS addresses there will be 1/10 success rate , and take precedence over the ISP's genuine DNS (the hacker proceeds to send the signal continuously). This is the way **DNS Cache Poisoning works** .

And because of the way it works, DNS Hijacking and DNS Cache Poisoning are used interchangeably.

3. How to prevent DNS Hijacking?

The best method is still:

1. Use a good and reasonable security software.

For simple users, **Avira Free Antivirus** is a great choice. Download the latest free Avira link:

1. Download Avira Free Antivirus

In the browser, restrict click on advertisements, especially when looking for crack software (a lot of malware comes):

1. How to block ads when using a browser

Try changing the DNS on your computer to Google's DNS ranges, Open DNS or Comodo DNS:

1. Google DNS: **8.8.8.8 - 4.4.8.8**
2. Open DNS: **208.67.222.222 - 208.67.220.220**
3. Comodo DNS: **8.26.56.26 - 8.20.247.20**

Good luck!

You finished reading the article "**Learn about DNS Hijacking and how to prevent it!**" 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.
