**Understanding DNS Hijacking**

Domain Name System or DNS acts as a phonebook and stores the IP address which is required to access a particular website. DNS Hijacking, also known as DNS redirection is a kind of cyber attack where the attacker attacks the DNS server by incorrectly resolving the DNS queries so that the user gets redirected to a website that is owned by the attackers. Cybercriminals hack the DNS either by changing the DNS server address or intercepting the communication between a user’s device and the DNS server. After the process of hacking, they replace the actual server IP address with their fraudulent site. For example, if someone tries to open [www.google.com](http://www.google.com), they will be redirected to the hacks page. Hackers can use the DNS hijacking or redirection attack to display advertisements or display a phishing website to steal confidential information from the user. They generate revenue by advertising or stealing the user’s money directly by infiltrating the bank account details or the credit card.

**Types of DNS Hijacking**

There are various types of DNS Hijacking. Below enlisted are the following.

**1. Local DNS Hijacking**

Hackers could use a trojan to replace the DNS server address on the user’s computer. The attackers change the DNS server meeting so that the user can be redirected to the hacker’s site.

**2. Router DNS Hijacking**

Cyber attackers can take advantage of the vulnerability in the router’s firmware and change the DNS server settings. Hijacking the DNS on the router level will affect all the users that are connected through that particular router.

**3. Man in the middle DNS hijacking**

In this type of DNS Hijacking, hackers intercept the communication between the user’s device and the DNS server. They catch the DNS server reply and replace the website server IP address and then send it back to the device. The user doesn’t suspect anything as the settings are accurate and the user believes the fact that they have entered the correct website URL.

**4. Rogue DNS Server Hijacking**

Attackers can directly attack the DNS server and redirect the users to fraudulent websites.

There is a prevalent confusion between DNS Hijacking and DNS Spoofing. Many consider both of them to be identical. Below mentioned are some features that differentiate the two.

DNS Hijacking or DNS redirection typically involves malware infection that changes the DNS settings on the user’s computer. The malware replaces the TCP/IP DNS server address with the malicious one. So all the DNS queries are sent to the hacker’s DNS server. They can redirect the user to the malicious server either by entering a specific domain or every time a user tries to access a site. On the other hand, DNS Spoofing is an act where the attackers spoof the DNS records. They can use DNS poisoning to spoof the local DNS cache on the computer. The hackers can also intercept the communication between the user’s pc and DNS server and spoof the DNS records. Also, attackers can hijack the DNS server and spoof the DNS records directly there.

**How to mitigate the risk?**

Getting protection against DNS Hijacking can be a little tedious. This is because several levels are involved in this type of attack. Hackers can hijack the DNS of the website and can easily redirect users visiting it. Also, they can hack the whole DNS server by changing the IP address of all websites. In this context, various steps are taken to minimize the risk of hijacking. Some of them are enlisted down below.

1)DNSSEC can be used to encrypt the communication between users and the DNS server.

2) Spoof detection tools and end-to-end encryption can be implemented to safeguard the users

3)Frequent checking must be done on devices to check for the presence of malware.

4)Passwords of the routers must be checked more often and installation of the latest firmware updates must be done.

**References**

1)<https://www.imperva.com/learn/application-security/dns-hijacking-redirection/>

2)<https://www.wallarm.com/what/what-is-dns-hijacking-basic-methods-of-protection>

3)<https://www.sentinelone.com/cybersecurity-101/dns-hijacking/>

4)<https://www.office1.com/blog/what-is-a-dns-hijacking>

5)<https://www.paloaltonetworks.com/cyberpedia/what-is-dns-hijacking>

6)<https://nordvpn.com/blog/what-is-dns-hijacking/>

7)<https://www.cloudflare.com/en-in/learning/security/global-dns-hijacking-threat/>