**Understanding DNS spoofing**

DNS is a system that converts the domain names into machine readable IP addresses for smooth functioning. But this system is targeted by cyber attackers for malicious activities. These attackers spoof the DNS server and send a different IP to the user which is infected by viruses and trojans.

**What is DNS spoofing?**

DNS spoofing is a kind of cybercrime in which the criminals misuse the DNS server to forward the user to a different IP address which is fake and harmful to the system, user, and also the sensitive and confidential data. Spoof means fake or imitation of something, which is the primary motive of the attackers. Criminals target this means to get access to users’ confidential and sensitive data, which by other means is a difficult target.

**Methods of DNS spoofing**

1)The most common method of DNS spoofing is to directly attack the DNS cache to redirect the users to a fake and malicious website containing the attacker's IP address which contains harmful viruses.

2)Another famous method is the Man in the middle (MITM) method where the attacker intrudes in the communication happening between two parties and misguides them by sending messages without the knowledge of the actual sender and receiver. According to them, they are communicating with themselves.

3)DNS cache poisoning is another kind of DNS Spoofing that targets the DNS cache and the data stored there.

**Risks of DNS Spoofing**

DNS Spoofing comes with its own risks and alarming effects. Given below are some of them.

1)Data theft is one of the very alarming risks that is faced by this type of attack. Personal and confidential data such as passwords, and ATM card pins are subject to danger when received by cyber criminals.

2)Removal of DNS cache poisoning is a problem as removing harmful malicious viruses from the cache is not a solution and doesn’t help in cleaning the system by any means. When uninfected systems are connected to servers that are already affected, they will be corrupted as well.

3)Due to the fewer security features of DNS and without any protection, attackers can use this medium easily for phishing purposes as well.

**How to prevent this?**

1)Use of VPN is a must as it provides good encryption.

2)Clicking on links that are not recognizable in the first place should be avoided.

3)Scanning tools should be present in the system so that regular scanning can be carried out to see the presence of malware if any.

4)Attached documents in emails without scanning should never be opened.

**References**

1)<https://www.myrasecurity.com/en/what-is-dns-spoofing/>

2)<https://www.javatpoint.com/how-to-prevent-dns-cache-poisoning-and-spoofing#:~:text=Use%20VPN%20(Virtual%20private%20network)%3A%20All%20the%20web%20traffic,much%20stronger%20against%20DNS%20spoofing>.

3)<https://heimdalsecurity.com/blog/dns-spoofing/>

4)<https://en.wikipedia.org/wiki/DNS_spoofing>

5)<https://www.cloudflare.com/en-in/learning/dns/dns-cache-poisoning/>

6)<https://economictimes.indiatimes.com/definition/dns-spoofing>

7)<https://www.infoblox.com/dns-security-resource-center/what-are-dns-spoofing-dns-hijacking-dns-cache-poisoning/>