**Understanding Cache Poisoning**

**What is Cache poisoning?**

Cache poisoning is a kind of cyber attack wherein the attacker injects false information into the DNS server so that the person using it gets misguided and lands on the wrong IP address.

This is a flaw in DNS where any individual or attacker can inject a malicious IP address into a name server. It tells people to go to a particular IP address instead of the actual one.

The attacker sends a request to the server. The query is then forwarded to the internet’s DNS and the attacker floods the local DNS with fake responses. The local server finds this malicious site in its cache and forwards the user to this malicious site.

**How does this occur?**

The primary motive of the attacker is to divert the users from the original IP address, thereby forwarding them to the wrong address. For this, they inject wrong information and fake IP addresses into the DNS cache. It is easy for attackers to attack DNS due to its weak points.

DNS uses User Datagram Protocol (UDP) instead of Transmission Control Protocol(TCP) for which they do not use the handshaking method for communication which is responsible for identifying the communicating parties and also for two-way communication. So, it is not possible to understand whether the sender is really the one they are claiming to be.

**Risks of Cache Poisoning**

DNS cache poisoning often comes with varied risks. Given below are some of them.

**1. Hindrance of data security and updates**

Due to cache poisoning, many necessary security updates can remain incomplete due to which the system is susceptible to harmful trojans and viruses.

**2. Malware Infection**

Attackers divert users to a different IP address which is infused with viruses. For this reason, attackers can readily install various harmful viruses.

**3. Data Violation**

When users get forwarded to another website that is harmful, sensitive and confidential data are subject to violence and hampering, like passwords, credit card information, etc. This violation happens without the prior knowledge of the user.

**How to prevent this?**

1. Users should never click on any unknown links as they might contain viruses.

2. Use of VPN is encouraged for end-to-end encryption.

3. All the systems must be regularly checked for viruses and malware and if any such is detected, it can be immediately canceled out.

4. DNS cache must be regularly flushed to keep it safe.

**References**

1)<https://www.techtarget.com/searchsecurity/definition/cache-poisoning#:~:text=Cache%20poisoning%20is%20a%20type,to%20a%20malicious%2Fdangerous%20server>.

2)<https://portswigger.net/web-security/web-cache-poisoning>

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

4)<https://www.sciencedirect.com/topics/computer-science/cache-poisoning-attack>

5)<https://www.acunetix.com/vulnerabilities/web/web-cache-poisoning/>

6)<https://www.networkworld.com/article/3298160/how-to-protect-your-infrastructure-from-dns-cache-poisoning.html>

7)<https://cybersecurity.att.com/blogs/security-essentials/dns-poisoning>