DNS cache poisoning

Introduction

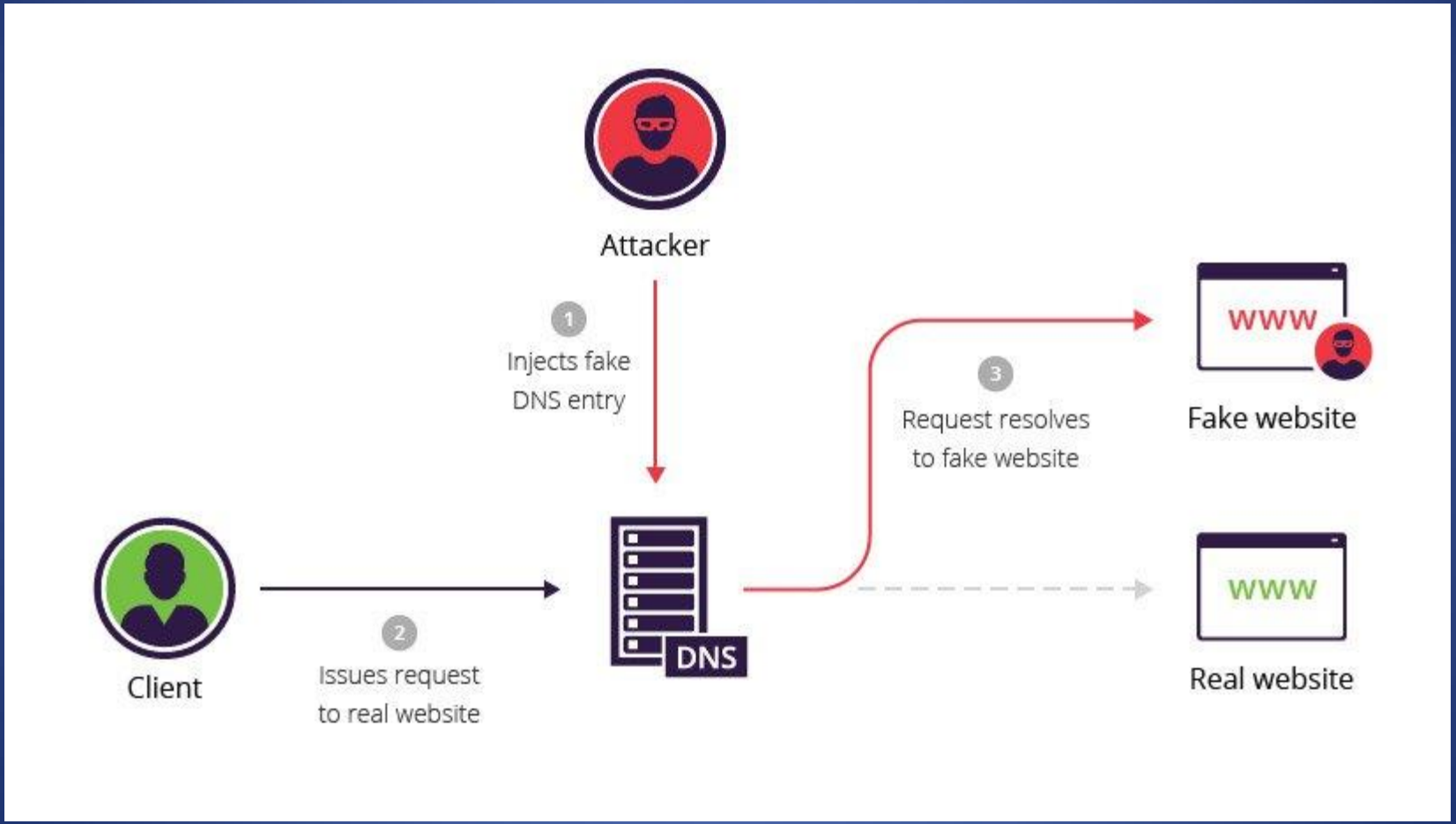
What is DNS cache?

We can make browsing faster by maintaining local DNS servers. They store the addresses of the websites in their cache memory. So that requests don't go to internet all the time. Whenever a requested address is not in cache, local DNS server forwards the request to internet (Master DNS Server) and diverts the user to the specific address.

What is DNS cache poisoning?

DNS poisoning is a type of attack in which hacker sends a request to local DNS server. Then this query is forwarded to internet (Master DNS server). In the mean time attacker floods the local DNS cache with fake responses. Whenever a normal user sends a request to the DNS server it directs them to malicious sites. These sites contain tools that steal user's data or harm their computer.

Example


Attacker
1
Injects fake
DNS entry
3
Request resolves
to fake website
www
Fake website
Client
2
Issues request
to real website
DNS
www
Real website

DNS Cache poisoning

Risks of DNS cache poisoning,

- Primary risk is theft of data. User's passwords, credit card information, and any other personal information is compromised.
- When the website is spoofed, user's computer may be exposed to additional threats such as Trojans and viruses.

Preventing DNS Cache poisoning,

- Configure it to be as secure as possible against cache poisoning by using a random source port, randomizing the query ID, randomizing domain names.
- DNSSEC.