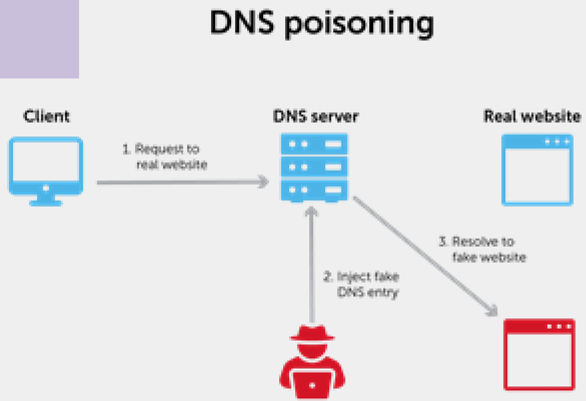
DNS Spoofing

CYSE 200T

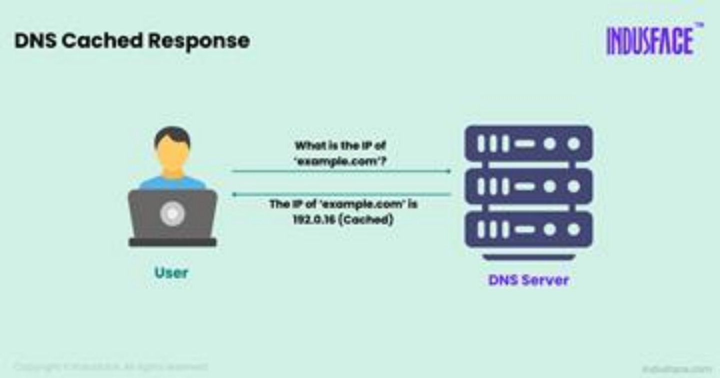


Adelina Bowden,
Kayla Nanton,
(Justin) Wilson

What is DNS Spoofing?

- DNS (Domain Name System) translates website names (like google.com) into numbers (IP addresses) that computers understand.
- The internet is like a phone book
- Imagine trying to call your best friend, but someone changed their number in your phone, and now you're calling a stranger!
- **DNS Spoofing** is when a hacker changes this translation, sending you to a fake website instead of the real one.

Different Ways DNS Can Be Tricked


DNS Cached Response
INDUSFACE
What is the IP of 'example.com'?
The IP of 'example.com' is 192.0.16 (Cached)
User
DNS Server

- **Cache Poisoning:** Corrupts DNS records stored in your device or router, leading users to fake websites.
- **Man-in-the-Middle Attack:** Hackers intercept and modify DNS requests in real time.
- **Rogue DNS Server:** Attackers set up a fake DNS server that always gives the wrong address.

How is DNS Spoofing Done?

3 types: Local, Router, and Server Poisoning

1. A hacker injects false DNS records into a DNS cache.
2. The next time someone types in a website, their browser is sent to the hacker’s fake site.
3. The fake site may look identical to the real one, tricking users into entering passwords, credit card details, or downloading malware.

Notable DNS Spoofing Attacks

- **Kaminsky Attack (2008):** Security researcher Dan Kaminsky discovered a serious flaw that made large-scale DNS spoofing possible.
- **Brazilian Bank Attack (2011):** Hackers redirected thousands of customers to fake banking websites.
- **MyEtherWallet Attack (2018):** Users of this cryptocurrency wallet were redirected to a fake site, leading to stolen funds.

How to Protect Yourself

- **Use Secure DNS Services** (like Google DNS or Cloudflare).
- **Enable DNSSEC** (prevents tampering with DNS records).
- **Avoid Public Wi-Fi** (and/or use a VPN).
- **Check for HTTPS & SSL Certificates** (a fake site may lack proper security).
- **Regularly Clear DNS Cache** (removes potentially poisoned records).
- **Enable Two-Factor Authentication** (even if credentials are stolen, access cannot be fully granted).

Risks of Public Wi-Fi Usage
keepnet
Data Theft
Man-in-the-Middle Attacks
Unauthorized Access
No Encryption
Malware Spread
Fake Networks

Conclusion

- DNS Spoofing tricks users into visiting fake websites.
- Hackers use various methods to Spoof such as cache poisoning and rogue servers.
- High-profile attacks have caused financial loss and data theft.
- Use security tools and best practices to stay safe!