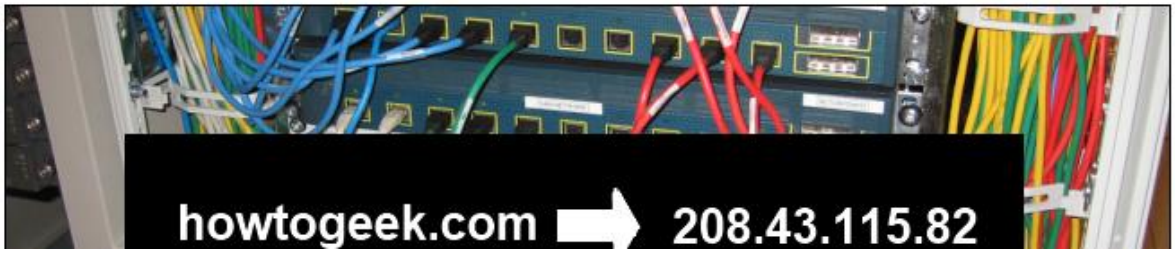
DNS cache poisoning, also known as DNS spoofing, is a type of attack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones.

One of the reasons DNS poisoning is so dangerous is because it can spread from DNS server to DNS server. In 2010, a DNS poisoning event resulted in the Great Firewall of China temporarily escaping China's national borders, censoring the Internet in the USA until the problem was fixed.

How DNS Works

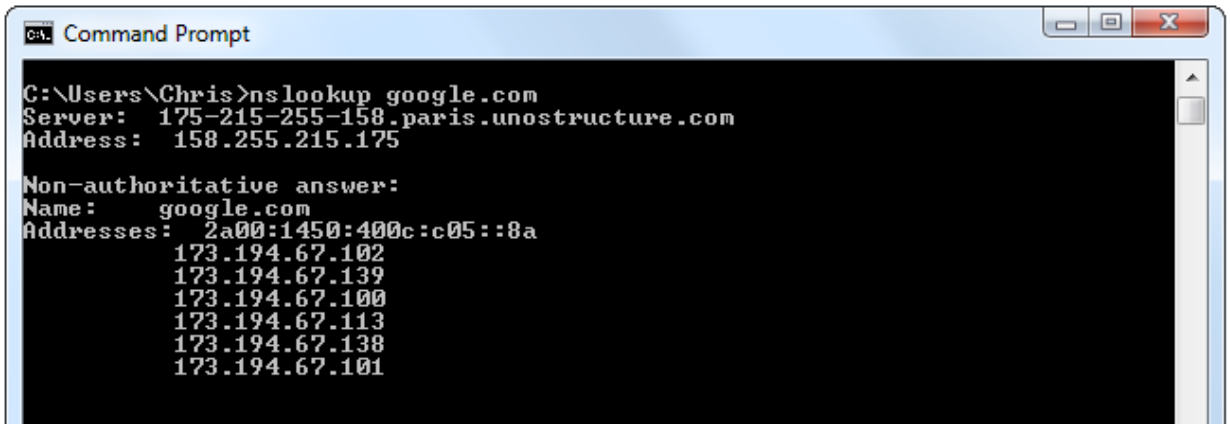
Whenever your computer contacts a domain name like "google.com," it must first contact its DNS server. The DNS server responds with one or more IP addresses where your computer can reach google.com. Your computer then connects directly to that numerical IP address. DNS converts human-readable addresses like "google.com" to computer-readable IP addresses like "173.194.67.102".

- Read More: HTG Explains: What is DNS?



DNS Caching

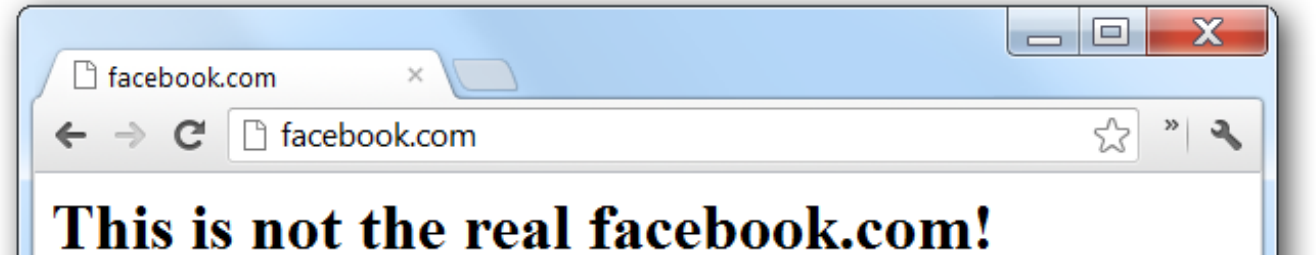
The Internet doesn't just have a single DNS server, as that would be extremely inefficient. Your Internet service provider runs its own DNS servers, which cache information from other DNS servers. Your home router functions as a DNS server, which caches information from your ISP's DNS servers. Your computer has a local DNS cache, so it can quickly refer to DNS lookups it's already performed rather than performing a DNS lookup over and over again.



DNS Cache Poisoning

A DNS cache can become poisoned if it contains an incorrect entry. For example, if an attacker gets control of a DNS server and changes some of the information on it — for example, they could say that google.com actually points to an IP address the attacker owns — that DNS server would tell its users to look for Google.com at the wrong address. The attacker's address could contain some sort of malicious phishing website

DNS poisoning like this can also spread. For example, if various Internet service providers are getting their DNS information from the compromised server, the poisoned DNS entry will spread to the Internet service providers and be cached there. It will then spread to home routers and the DNS caches on computers as they look up the DNS entry, receive the incorrect response, and store it.



The Great Firewall of China Spreads to the US

This isn't just a theoretical problem — it has happened in the real world on a large scale. One of the ways China's Great Firewall works is through blocking at the DNS level. For example, a website blocked in China, such as twitter.com, may have its DNS records pointed at an incorrect address on DNS servers in China. This would result in Twitter being inaccessible through normal means. Think of this as China intentionally poisoning its own DNS server caches.

In 2010, an Internet service provider outside of China mistakenly configured its DNS servers to fetch information from DNS servers in China. It fetched the incorrect DNS records from China and cached them on its own DNS servers. Other Internet service providers fetched DNS information from that Internet service provider and used it on their DNS servers. The poisoned DNS entries continued to spread until some people in the US were blocked from accessing Twitter, Facebook, and YouTube on their American Internet service providers. The Great Firewall of China had "leaked" outside of its national borders, preventing people from elsewhere in the world from accessing these websites. This essentially functioned as a large-scale DNS poisoning attack. (Source.)