DNS hijacking

It is a serious threat to the system and can have very costly consequences. As the attack allows a cybercriminal to take control of the DNS settings and redirect users to fraudulent websites, this can affect many different users. DNS hijacking involves changing the DNS settings themselves, often by installing malware on victim computers. This allows the hacker to take control of routers, intercept DNS signals or simply hack DNS communications.

How does it work?

The DNS system works by translating human-readable domain names into numeric IP addresses that computers use to communicate. When a user enters a web address, the browser queries DNS servers to obtain the corresponding IP address. The vulnerable point is the unencrypted communication between the browser and the DNS server in traditional DNS queries (without security extensions such as DNSSEC).

Types of DNS hijacking.

- Local hijacking: The hacker installs a malicious Trojan on the system to attack the local DNS settings. After the attack, you can change these local settings to point directly to your own DNS servers.
- Router hijacking: This is often the first point of attack for many cybercriminals. This is because many routers have default passwords or existing firmware vulnerabilities, which hackers can easily find. Once inside, they modify the DNS settings and specify a preferred DNS server.
- Fraud hijacking: Cybercriminals hijack the ISP's existing nameserver to change selected entries. As a result, unsuspecting victims seemingly access the correct DNS server, which was actually infiltrated by hackers.