



CLEVER® Solutions Empowering Global Enterprises

I recently almost got spoofed while submitting my authentication info on one of my accounts. Fortunately, I noticed the odd, misspelled URL, before clicking the Submit button. The attacker has already gotten control of this service's DNS server, redirecting traffic to their malicious websites. Service providers should not count on the end-users to detect any breaches. There must be a better way.

Remediation is very difficult once your DNS cache is corrupted, your authoritative DNS server possibly poisoned, and your DMZ host possibly compromised if you have one. The longer they are in your network doing reconnaissance, and hijacking traffic, the more costly it would be.

Attackers may use DNS for both external and internal reconnaissance, to hijack the traffic, and to create covert communication channels. Needless to say, it serves to proactively fortify your DNS servers with the followings:

- Take the added step of verifying DNS data with public-key cryptography verification (DNSSEC).
- Enable secure DNS configurations.
- Always encrypting data included in DNS requests and answers.
- Update so that you use the most recent DNS version.

Securing the enterprise operation requires the best monitor to look for certain warning signs. Two of the biggest warning signs are (1) an increase in DNS activity from a single source about a single domain, which can indicate a **BirthDay attack**, and (2) an increase in DNS activity from a single source about multiple domain names, which can indicate attempts to find an entry point for DNS poisoning.

CleverDetect® for DNS provides the real-time **DNSDiff™** function to ensure the data integrity of your critical DNS records. It will alert you whenever there's a change in your DNS records due to possible malicious attacks or misconfigurations. It will also monitor the health of your DNS service for availability and performance.

Mark
CTO

Learn More About [CleverDetect for DNS](#) and [AES CLEVER Family of Products](#)

[Free Trial](#)

[Webinar](#)

[Website](#)

[Email](#)