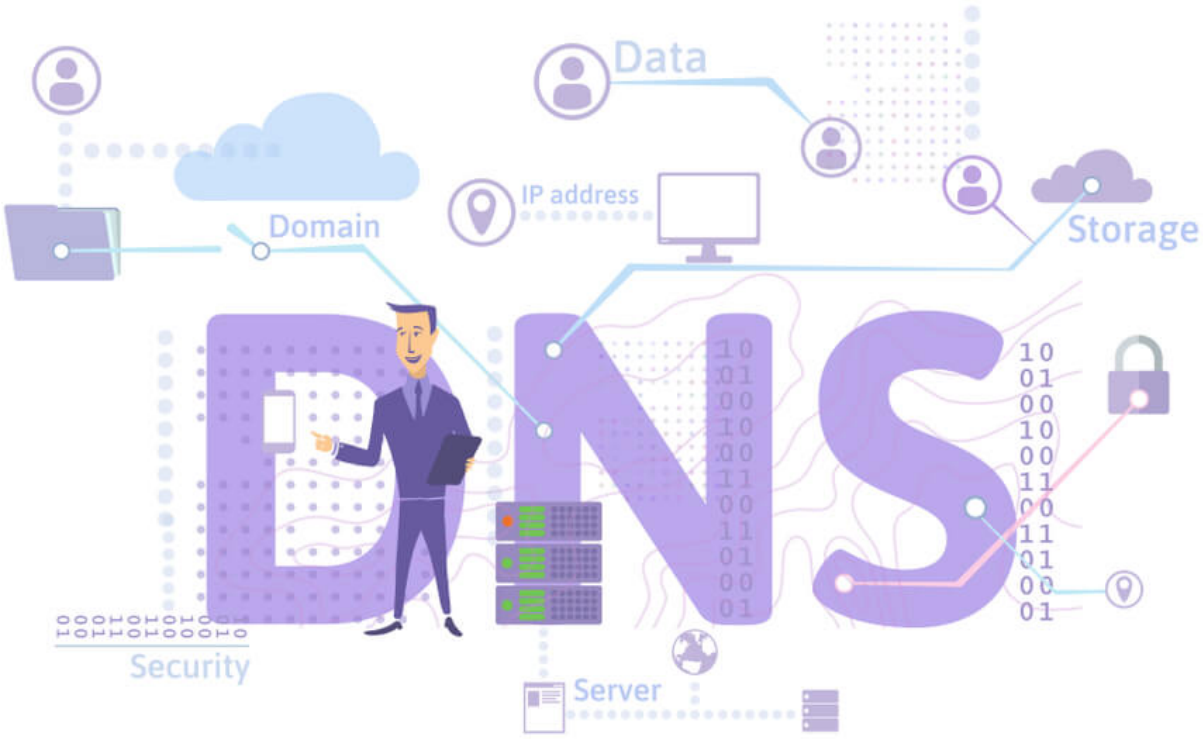
Take Control of Nameserver Records with a Reverse Nameserver Lookup API

Posted on January 10, 2020



One reason why cyber risks are far more serious today than in the past is the widespread and cheap access to services from registrars and hosting providers. From amateur bloggers to small business owners, anyone can register a domain and create a website for whatever purpose.

The problem is that not everyone has the right skills to properly configure servers — e.g., define hosts or set up address (A) or pointer (PTR) records, among other things.

Website owners are lucky if issues from nameserver misconfigurations only result in reduced website availability. There are other consequences, though, such as higher spamming scores and Secure Sockets Layer (SSL) authentication errors or vulnerabilities that could potentially lead to security compromises.

Let’s take a look at why NS records and Domain Name System (DNS) credentials should be adequately managed to avoid cyber attacks and the roles of tools such as Reverse NS API in tackling security challenges.

What Nameserver Records Reveal About Your DNS Posture

Understanding what happens under the hood is part of website housekeeping, which is mostly concerned with your domain’s DNS records that operate on trust anchors. At the most basic level, DNS records play a crucial role in how devices communicate over the Internet.

The DNS translates “human-readable” resources or domain names stored in nameservers into IP addresses assigned to network devices or nodes (“direct” translation) — and the other way around, from IP addresses to nameservers (“reverse” translation).

There are different DNS record types, but the most crucial ones are the A, CNAME, nameserver, and mail exchange (MX) records. These resources resolve to an IP address assigned to a particular device. (For a more in-depth explanation of DNS records, read our Domain Name System Primer.)

Why It's Important to Keep Your Records Accurate and Updated

Assuming that records are where they should be and that your provider is fine, you shouldn't encounter any problems. However, NS records may be accidentally overlooked, abandoned, or misdirected during website migration or when you change providers. Nefarious actors could also falsify your records or trick you into changing them through techniques such as:

DNS Record Dangling

Using dangling pointers for exploit attacks can be child's play for experienced hackers. Domain owners sometimes forget to clean up their A or CNAME records when they change IP addresses or give up expired domains. Then, cyber attackers can effortlessly reserve and acquire floating IP addresses and dangling DNS records. Once they do, they can take over the domains those previously pointed to.

Believe it or not, dangling pointers abound on the Web. A significant number of active MX servers used by highly reputable domains point to expired locations.

NXDOMAIN

A non-existent domain (NXDOMAIN) message is triggered when a domain cannot resolve to an IP

address, which happens when a user queries an expired or misspelled domain name. However, high rates of NXDOMAIN responses may indicate that bots are using the domains in question via a domain generated algorithm (DGA) to communicate with command-and-control (C&C) servers. Additionally, hackers and some Internet service providers (ISPs) frequently exploit the NXDOMAIN condition to hijack DNS servers to redirect traffic to bogus sites.

Social Engineering

Attackers may impersonate registrars or IT administrators and send phony requests to victims to hijack NS records through phishing emails and other fraudulent communications. They may also lure email receivers to malware-infected links and attachments that could corrupt server files or steal credentials.

How Reverse Nameserver Lookup Tools Help

Below are ways in which infosec professionals can gather actionable threat intelligence by a **lookup of nameservers**.

Cross-Referencing Data

Threat actors can easily forge or alter DNS records. However, most WHOIS records list authoritative nameservers that you can use for verification. Reverse NS API can reveal unrelated or hijacked domains connecting to your nameservers. Should inconsistencies exist between your nameserver information on record and in the DNS, a passive DNS lookup can be subsequently performed to determine if and when changes were made.

Identifying C&C Servers or Blacklisted Nameservers

Incorrectly configured domain nameservers and hosts that communicate with malicious servers may result in NXDOMAIN responses. You can cross-check whether a domain you own is misconfigured or associated with a known C&C server or a blacklist when you run a reverse **nameserver lookup**. The results would allow you to query nameservers to pinpoint IP addresses that you should block.

Preventing DNS Infrastructure Leaks

Reverse **nameserver lookup** tools come in handy in spotting misconfigured DNS zone transfers that could leak your entire DNS database. The resultant dump from a DNS leak may reveal valuable information, such as that on other subdomains and their nameservers, which hackers can individually assess for weaknesses.

Effective DNS Management and Audits

Reverse **nameserver lookup** applications empower security professionals when integrated into DNS traffic monitoring systems. They can greatly enrich alerts generated by your security information and event management (SIEM) solutions.

Good threat intelligence is the foundation of a robust DNS management program. Through the data points it provides, Reverse NS API can mitigate the risks brought on by insufficiently secured DNS records.