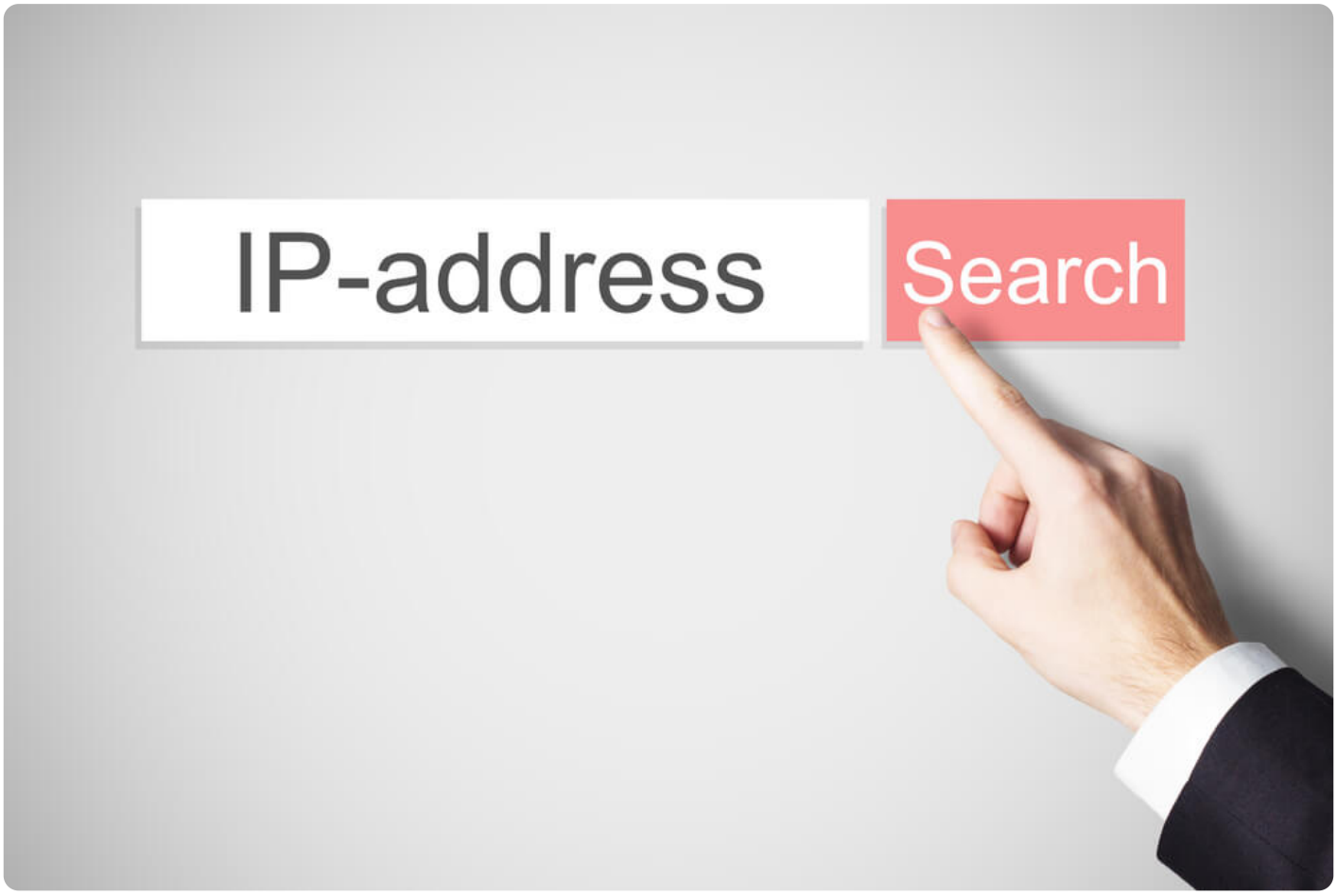
How a Reverse IP & Domain Lookup Can Save Organizations from Stale DNS Records

Posted on January 30, 2020



Every website that can be accessed on the Internet comes with an IP address that points to a specific domain name. Each domain-to-IP address mapping is recorded in the Domain Name System (DNS), which makes it possible for users to not have to remember numeric addresses to reach a particular website while still letting DNS resolvers do their matchmaking work. And for this to happen, a DNS record contains many crucial details about a website accessible via the World Wide Web.

Unfortunately, when a website ceases to exist, its owner may forget about its DNS records. These records are what is known as “dangling” or “stale” records, which attackers often abuse as part of their nefarious schemes.

What Are Stale DNS Records?

In simple terms, a stale DNS record is a record that is no longer in use and hasn’t been refreshed for a while but is still connected to one’s DNS infrastructure. Because they have aged and are often left forgotten, stale DNS records have become potential IoCs that cybercriminals can scavenge and take control of.

Stale DNS records may emerge from different scenarios. One of them, for example, is when a subdomain was created with its own DNS record for testing updates and new features locally without interfering with the main live site. Once all is working fine, developers may then apply the changes in the production environment. But they may forget to decommission the testing site and its DNS record — which then becomes “stale” but remains an active component that can end up being exploited.

What Do Cyber Attackers Use Stale DNS Records For?

Stale DNS records pose no danger if the one who finds them has no malicious intentions against

their owners. That changes, however, when the ones who discover them are cybercriminals. Most cyber attackers use stale DNS records to launch so-called subdomain takeovers. Here are some of the most popular subdomain takeover attack types:

- **Mail exchanger (MX) subdomain takeover:** MX records are essential as they ensure that an organization maintains smooth email functionality. An MX record points emails meant for a company to the right mail server. Attackers can manipulate stale MX records to point instead to a mail server under their control so they can get the messages meant for the target organization. These emails can contain confidential information that the attacker can harvest. He can also target the senders for a spearphishing campaign.

- **Canonical name (CNAME) subdomain takeover:** A CNAME record maps an alias to the true or canonical domain name. This attack is possible when an alias for a CNAME is available for registration. Many domain owners sometimes forget to renew registrations on aliases while leaving their records intact. When an attacker finds them, however, he or she can register and take control of it. If it still points to its original network, the attacker essentially gets one foot in the door. He can then move inside the network by exploiting vulnerable systems or carry out man-in-the-middle (MitM) attacks.

- **Name server (NS) subdomain takeover:** An NS record indicates which DNS server is a domain's authoritative server. While an NS subdomain takeover is not as common as a CNAME subdomain takeover, it remains a threat. An attacker can take control of a domain's authoritative DNS server to redirect all traffic to his chosen site.

How Can a Reverse IP & Domain Lookup Help Prevent Subdomain Takeovers?

Mitigating subdomain takeovers with a reverse IP domain lookup tool like Reverse IP/DNS API is pretty straightforward. Running a **reverse IP** & **domain** search on your property allows you to see all of the domains hosted on your IP address. If you notice an unknown domain, you can investigate it immediately. And if it proves suspicious or outright malicious, sever all ties to it.

A **reverse IP** & **domain lookup**, powered by a DNS Lookup API, also shows all of your domain's DNS records. You can carefully scrutinize those for anomalies and immediately fix issues (e.g., stale DNS records) before attackers can abuse them.

More specifically, domain owners have two options when dealing with stale DNS records. These are:

- **Claiming the domain names they point to:** To do this, you can register the resource with a cloud service provider or repurchase the expired domain if it is a regular Internet domain.

- **Deleting the dangling DNS record:** This is the more efficient way of preventing subdomain takeovers, particularly if your organization does not see a need for the affected domain. Deleting stale DNS records disassociates the resources on them from your network.

Doing a routine audit of your domains and subdomains with **reverse IP/domain lookup** tools such as Reverse IP/DNS API and DNS Lookup API allows your organization to maintain the integrity of your DNS infrastructure. This process lets you, among other aspects, rid your network of stale DNS records that cyber attackers might potentially abuse.