How to Look Up an ARIN IP Address with IP Netblocks WHOIS Database

Posted on April 2, 2020

Why does it matter who's behind an IP address? Knowing the identity of IP addresses' owners, whether they are individuals or organizations, helps users determine if they can be trusted or are potential scammers out to carry fraud.

However, that information is not always readily available, and nor is it publicly accessible due to a variety of reasons. So, how can users obtain such data? One resource that may help is an IP Netblocks WHOIS Database. In a nutshell, it lets users know what IP netblock or range an IP address belongs to and who owns it.

This post discusses how users can find an American Registry for Internet Numbers **(ARIN) IP address** by using an **IP netblock database**. But first, let's find out what ARIN is.

What Is ARIN, and Why Is It Important?

Five regional Internet registries (RIR) are tasked by the Internet Assigned Numbers Authority (IANA) to assign IP ranges to Internet service providers (ISPs). These providers then assign IP addresses or, in some cases, entire blocks to entities, both individuals and companies alike.

One of these five RIRs is ARIN, which designates IP addresses to entities in the U.S., Canada, and certain parts of the Caribbean. On its website, ARIN highlights the importance for entities that apply for IP netblocks to provide accurate and updated information, specifically their points of contact (PoCs). For companies, the PoC can be its system administrator who is responsible for maintaining their IP addresses.

RIRs ask entities to provide valid contact details in case attackers use their IP addresses fraudulently. In some instances, cybercriminals target the IP addresses or ranges of entities that do not keep their records up-to-date. That is not surprising as such organizations may also not closely monitor their IT assets.

RIRs also keep contact details at hand in case law enforcement agencies ask for these for their

investigations.

Benefits of Using an ARIN IP Address Lookup Database

Most **IP Netblocks WHOIS database** providers offer downloads by region. For companies that only deal with clients or customers from specific countries, that is beneficial since a regional database would cost less than a global one. That said, users looking for information on entities with ARIN IP addresses can opt to download a regional database.

Unlike a WHOIS/IP database, IP Netblocks WHOIS Database goes beyond telling users about who owns an IP address. They can also get other information from it, primarily the IP range an address belongs to and its abuse contact details. These are critical bits of information for users who want to keep their network and confidential data safe from attacks.

Let us say that you are part of a clothing manufacturer's IT security team and found that the U.S.-based IP address 107.151.209.99 is attempting to access an internal-only system on your network. You can consult an **ARIN WHOIS IP** database to find out who owns it. You should be able to get these details:

- The IP address is part of the range 107.151.209.96–107.151.209.103.
- The company VpsQuan LLC located in Yining, China, maintains it.
- Its abuse contact email address is admin@vpsquan[.]com.

Knowing this about an IP address, users can:

- **Report abuse to the owner of the range:** Cybercriminals are known for spoofing someone else's IP address in attacks to throw off the scent during investigations. You can contact the IP address's owner via the abuse contact email address to resolve an issue as a first step. Its owner may not know that it figures in an attack. The IP address may also belong to your

trusted contact and that is why he or she is attempting to access your protected system. If the address, however, does not belong to anyone your organization trusts, block it so it cannot compromise your security, especially if it turns out to be under a threat actor's control.

- **Identify connected IP addresses and domains:** Several lists of IP addresses used in attacks are publicly accessible. Armed with such a list, users can create abuse history profiles to determine if an IP address should be blacklisted or further investigated. We know, for instance, that the U.S.-based IP address 96.44.183.146 has been reported several times. After blacklisting it, you can use an **ARIN WHOIS IP** database to get more insights into the range it is part of. You will know that it is part of the block 96.44.182.0–96.44.183.255, which belongs to QuadraNet, Inc. While most companies don't block entire ranges from accessing their networks, should more IP addresses from the range figure in attacks, the blocking of it may be an option. To find out more about a specific IP address such as the domain it is associated with, you can use Reverse IP/DNS API. Monitoring its owner via Reverse WHOIS API for malicious ties is also advisable.

IP Netblocks WHOIS Database is a powerful asset offering a wide array of information that is useful for IP intelligence gathering. For more information on how you can harness its benefits to learn more about ARIN IP addresses, contact us at support@whoisxmlapi.com.