How to Find a Netblock Owner with an IP Netblocks WHOIS Database

Posted on January 27, 2020

IP netblocks can be considered a neighborhood to which consecutive IP addresses belong. As in the real world, there are good and bad neighborhoods. Fortunately, sophisticated threat intelligence tools enable security engineers to distinguish one from the other.

Traditionally, users can check computers communicating over a network by using a simple ping command to find unresponsive or misbehaving nodes. A ping test sends packets to a server and reveals if the same number of packets were returned, as well as how long it took the destination to issue a response.

Ping tests may be sufficient for network discovery, especially in private networks. However, other tasks may require critical IP intelligence data, such as a **WHOIS IP block**, for threat hunting and marketing applications. An IP Netblocks WHOIS Database can provide complete ownership histories of IP ranges that can help users determine if these were involved in previous attacks.

Use Cases for an IP Netblocks WHOIS Database

Public network data is useful for companies that wish to steer clear of privacy violations. Below are some typical applications of IP netblocks data supplied by our database:

- **Host discovery:** Netblocks information provides network engineers with immediate data on malfunctioning or disconnected devices. It also helps them determine domains and IP addresses on a dedicated or shared server.

- **Cyber forensics:** Threat hunters can rely on the IP Netblocks WHOIS Database to pinpoint blocks related to offending IP addresses, effectively ban them, and alert their abuse contacts. Additionally, they can use netblocks as a starting point for investigating domain names with large footprints.

- **Security incident and event management (SIEM) data enrichment:** Cybersecurity professionals can add context to indicators of compromise (IoCs) with subnetwork

information. By cross-referencing netblocks data, analysts can reduce false positives that could otherwise waste time and resources.

- **Enterprise sales and marketing:** An IP Netblocks WHOIS Database provides companies like hosting or cloud storage providers information on available netblocks that they can purchase when they're ready to scale up. They can also use netblock records to examine IP routing data for market or competitor research (i.e., to predict how much of the web traffic a company receives converts to sales).

- **Supply chain risk management:** Cyber risk assessors can use WHOIS IP blocks records to correctly validate bulk traffic originating from third parties through shared logistics or inventory systems. Meanwhile, organizations can map out their infrastructure from the real world to IP netblocks to ensure the integrity of their networks.

How to Use an IP and WHOIS Database to Search for IP Netblocks

Here are the steps to find an IP range and its owner using our IP and WHOIS database:

- Download the **IP block** data feed in .csv format via Hypertext Transfer Protocol Secure (HTTPS) or File Transfer Protocol (FTP).

- Choose a program that best suits your requirements. Sifting through a large .csv file may work for some users, but cybersecurity teams who deal with large datasets may prefer other arrangements. You can, for instance, build your own relational or non-relational database management system like MySQL or NoSQL based on the ready-made database solutions we offer on GitHub.

- Type in the command or script to load the .csv file to your database or software. You can view a sample of this exercise here.

- Interpret the output based on the descriptions from our specifications page. The most

commonly used values for IP netblocks analysis are:

- **inetnum:** This refers to the IP range a company owns.
- **as number:** Autonomous System (AS) numbers refer to the IP prefixes used by network operators or organizations for its routing system. These numbers correspond to the geolocation of a specific netblock and can be queried to easily determine the company name and maintainer if that is missing or masked.
- **netname:** This refers to the name of the IP block owner.
- **modified:** The last modified date can tell users when a netblock was created or changed hands.
- **country/city (in separate tables):** The country and city associated with a netblock. Example outputs would be a two-character country code, “US,” and a spelled-out city name “BOCA RATON,” such as for one of Verizon’s netblocks.
- **maintainers:** Refer to the people who have the right to make changes to an IP range. The output comes in the form of a code or an ID.

More details about maintainers and contacts can usually be found in the Contacts file. Additional queries may be done either through the IP netblocks database itself — which simplifies the process — or externally. For instance, users can look up the primary key, “PHIX-NOC-AP,” on the Asia-Pacific Network Information Centre (APNIC) WHOIS Database to retrieve the full names, physical locations, and email addresses of its associated maintainers.

Netblocks data is an indispensable component of any cybersecurity or marketing professional’s toolset. IP intelligence solutions like IP Netblocks WHOIS Database allow analysts and marketers to evaluate domains and network blocks nearly in real time, without having to consult an overwhelming number of records.