Why You Need an IP Netblocks WHOIS Database for IoC Enrichment

Posted on June 10, 2020



Indicators of compromise (IoCs) are anomalous network or computer artifacts such as malware signatures, file hashes, or domains that point to a possible breach. This data is aggregated from multiple external threat feeds and log files from internal applications and systems. The analysis of IoCs is part and parcel of an infosec professional's daily workload. After all, an organization's security hinges on its ability to detect and act on IoCs that could lead to full-blown cyber attacks timely.

Every day, analysts encounter IoCs of varying severity, as reported by their organization's security orchestration, automation, and response (SOAR) and security information and event management (SIEM) solutions. The problem with such alerts is that some may be associated with old IoCs that are no longer active or are now being used for legitimate purposes.

That explains the need for constant IoC management. By monitoring IoCs in context, security analysts can find out which ones warrant their attention most as the volume of alerts can easily overwhelm an understaffed security team. But was does "context" mean here? And which sources of data can support in providing it?

Among other data feeds, IP Netblocks WHOIS Database can ease the burden of IoC enrichment activities for analysts. Let's find out how.

How an IP Netblocks WHOIS Database Helps with IoC Enrichment

One way to enrich IoCs is to look for associations between them and the entities responsible behind. In the context of this blog, this includes domain registrants, Internet service providers (ISPs), and hosting companies. The next step is to correlate the findings from that exercise with threat intelligence information.

IP Netblocks WHOIS Database enables users to retrieve the ownership data of IP address ranges as well as the entire hierarchy of the netblocks an IP belongs to (from the whole Internet to the smallest contiguous range assigned to some entity). For an introduction to the notion of netblocks and IP whois, check this blog post.

With IP netblocks, users can better validate an IP address's nature by learning more about the

organizations, such as the regional Internet registry (RIR) and ISP that issued them, along with the other IP addresses in its “neighborhood.”

IP Netblocks WHOIS Database helps explicitly with the following:

1. Reconnaissance

IP Netblocks WHOIS Database helps users put together the tools, tactics, and procedures (TTPs) employed by attackers by adding context to IoCs associated with campaigns. It allows users to locate the threat actors targeting their organizations, spot trends, and identify malicious resources by providing IP range ownership information. The database contains a range’s Autonomous System number (ASN), organization, city, state, and country of origin, among other data points.

Say you encounter the IP address 176[.]34[.]241[.]253, which is a malware host connected to the domain coronavirus[.]com, in your logs. With IP Netblocks WHOIS Database, you can find out who currently maintains it. We obtained the following details, for instance:

Autonomous system (AS) number

ASN: 16509

Name: Amazon.com

Route: 176.34.192.0/18

Domain: http[:]//www.amazon[.]com

Type: Enterprise

Netname: AMAZON-EU-LHR2-AWS

Modified: October 2, 2019

Country: NL

Administrative contacts

ID: ADSI2-RIPE

Role: Amazon Data Services Ireland Technical Role Account

Email: ripe-interest@amazon[.]com

Address: Amazon Data Services Ireland, Digital Depot, Thomas Street, Dublin 8, Ireland

With the IP address's issuer, RIR (Réseaux IP Européens [RIPE]), and contact details at hand, users can request the ISP or RIR to take the offending IP address offline. Users can also opt to block the range that the IP address belongs to, but they should proceed with caution as it could lead to overblocking.

2. Threat Analysis

IP Netblocks WHOIS Database enables users to analyze IP addresses and correlate them with specific organizations and geographic regions. Information gleaned from the database allows users to build attack hypotheses and pinpoint the source of attacks accurately so they can triage an incident promptly.

Let's take the suspicious IP address, 185[.]220[.]100[.]240, which was flagged as a high-risk number resource by a cyber risk assessor as an example.

The database yielded six IP ranges in its neighborhood that belong to a Bavaria-based nonprofit Internet infrastructure company called "F3 Netze." The company, which operates servers for Tor network users, assigned the address as an exit node. As far as we know, utilizing Tor is not typical corporate practice. It may thus be a good idea for affected organizations to block the access of similar IP addresses or ranges across their networks.

An organization's risk profile changes as time goes on. IoCs that you encountered once are likely to be no longer valid today. Still, bringing context to IP data can assist your team in understanding embedded threats in your network, as well as those hiding behind external hosts.

As shown in this post, IP Netblocks WHOIS Database among other data feeds can provide users with the necessary information to enrich their knowledge about threats so they can respond or thwart them on time.