IP Source

What

In 2023, servers on the internet are constantly pinged for vulnerabilities. Millions of bots scan the internet for information to steal, for framework info to exploit, for open databases with tables of user data waiting to be stolen and so on. Identifying these attackers is critical for the security of the internet.

Luckily there is a Yellow Pages for the internet. Unfortunately for us, obtaining the data is relatively difficult. There are 5 regional "masters of the internet" that are given the ability to assign IP blocks to ISPs. They each give us a list on an FTP server full of allocated IP addresses.

This is it however. Any data behind who this IP address belongs to and the contacts at the company who owns it is strictly through an API called "RDAP". This API has a relatively low rate limit so gathering the data is difficult.

For our "Big Data" solution, we can download the 5 lists from each regional IP address god, throw the beginning IP in a queue and then have consumers that use a proxy network to download the hundreds of thousands of IP addresses and their owner's info and save it to our database to identify the network which includes "abuse" contact information.

This product is geared towards cybersecurity teams who wish to identify the network owner of malicious traffic to reach out and ask the network owner to block the traffic.

The product is unique in the regard that not many services offer this. One service that does come to mind is IP Info. The product is unique in the sense that it gets the data directly from the source of the data using a clever distributed worker trick behind a rotating proxy.

How