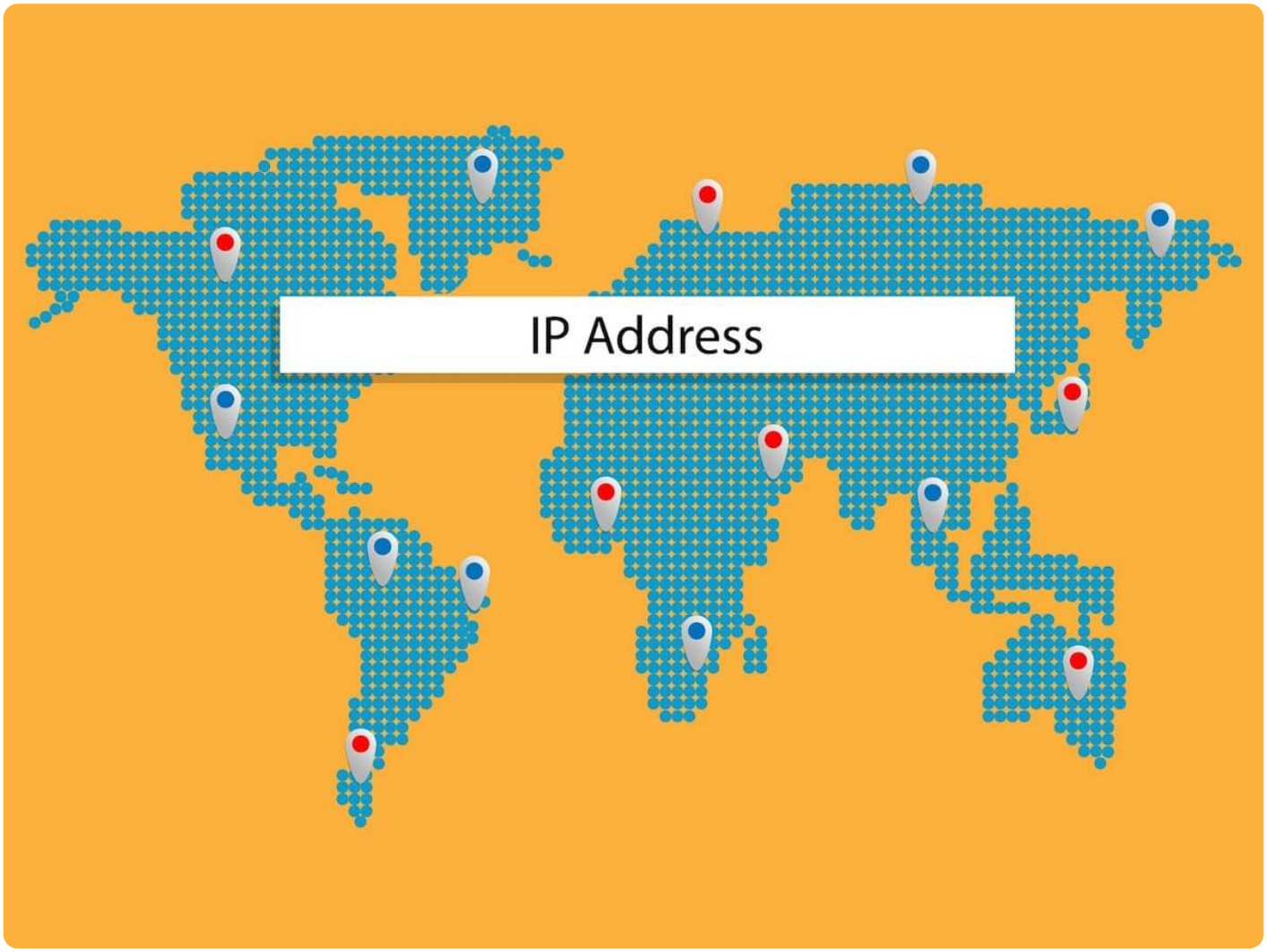
IP and WHOIS Database: How to Find APNIC Block Owners

Posted on February 27, 2020



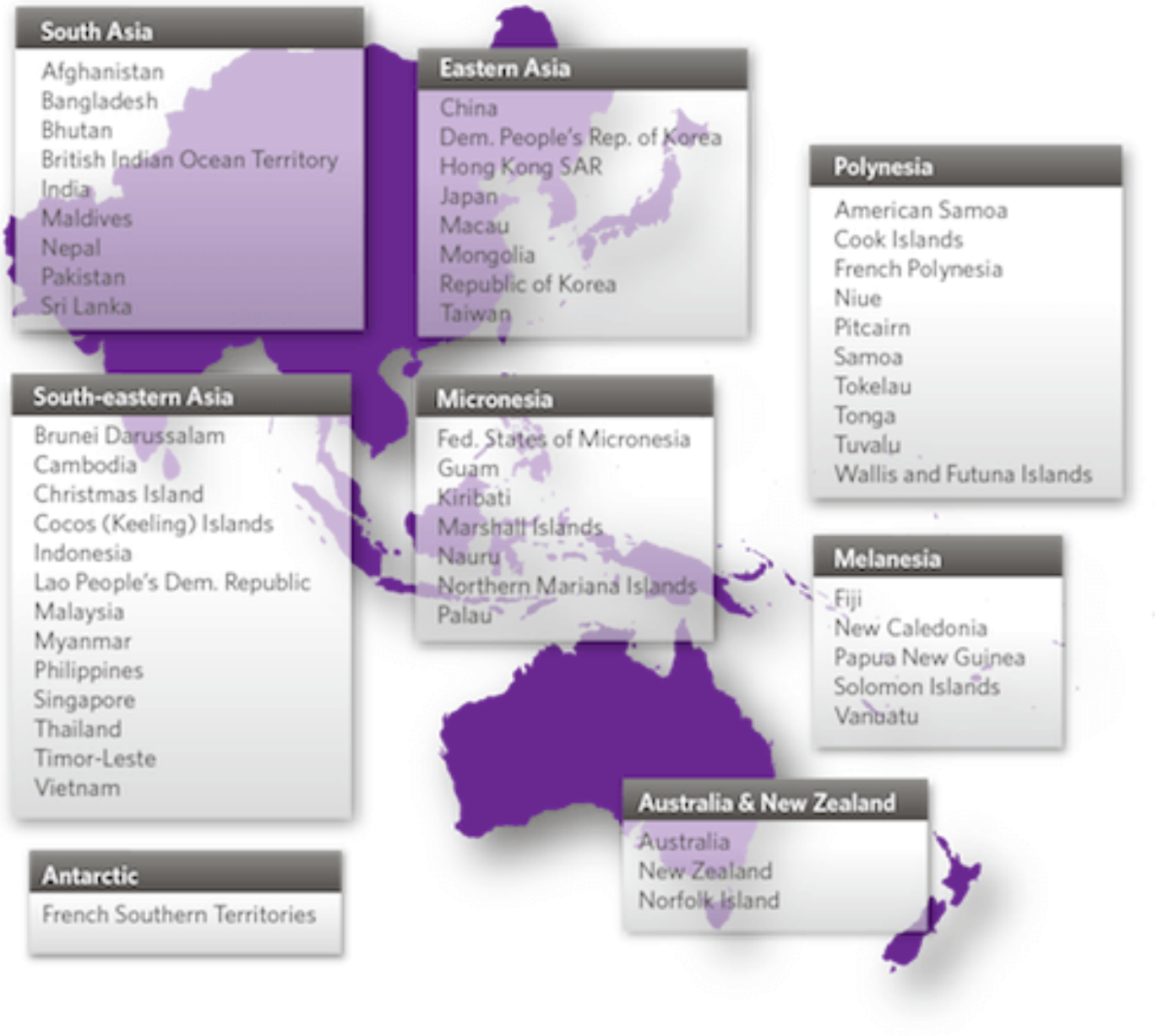
In the 1980s, detectives, investigators, and regular people who wanted to solve a mystery would need to sit in a car for hours, wear a disguise, and follow their subjects everywhere, be it on foot or by car.

The nature of crimes, however, has changed today. Most of them no longer happen physically; they're committed in the virtual realm. And so, they call for new methods of investigation where legwork (in the physical sense, that is) is no longer required. Tracing the identity of a cybercriminal, for instance, now requires the right information and sources like an IP WHOIS database.

In this post, we delve into the methods and tools that can help users find the owner of an Asia Pacific Network Information Centre (APNIC) IP block in particular.

What Is an APNIC Block?

First, let us delve into what APNIC is. APNIC is a non-profit organization tasked to manage and distribute IP addresses and Autonomous System (AS) numbers in the Asia Pacific region, which includes the countries shown in the image below.



Source: APNIC

APNIC assigns IP addresses to Internet service providers (ISPs) and other networks by “block.” The sizes of the blocks differ and seen after an oblique (/). So, the IP range 59.154.0.0/16 contains about 65,000 IPv4 addresses from 59.154.0.0 to 59.154.255.255.

An APNIC block is, therefore, a range of IP addresses that belongs to a network within the Asia Pacific region.

How Can an APNIC Block Owner Be Traced?

You can track down the owner of an APNIC block if you have access to an APNIC IP database. In fact, you can use our IP Netblocks WHOIS Database, which contains over 9.1 million IP netblocks, including those managed by APNIC.

With a given IP address, you can find the IP range it belongs to, along with its owner’s details. One way to do so is by downloading the database in JSON or CSV format via HyperText Transfer Protocol Secure (HTTPS) or File Transfer Protocol (FTP).

Let’s say you want to trace the owner of 59.154.0.0/16, the IP range mentioned earlier. IP Netblocks WHOIS Database showed that it pertains to SingTel Optus, one of the leading telecommunications companies in Australia. Among the ownership details gleaned from the database are the following:

- **Domain:** http://optus[.]com[.]au/business
- **Address:** Optus Macquarie Park, 1 Lyonpark Road, Macquarie Park NSW 2113
- **Admin contact email:** ipadmin@optus[.]net[.]au
- **Admin contact phone:** +61 2 8082 7800

Aside from IP Netblock WHOIS Database, you can also use IP Netblocks API. It derives data from

the same IP WHOIS database and provides results in XML or JSON format.

Why Is It Important to Trace IP Netblock Ownership Details?

There are several reasons why you may want to trace the owner of an IP netblock, ranging from cybersecurity and network filtering to preparing for an acquisition. We listed some of them below.

Investigating a Cybercrime

Cybercriminals use malicious IP addresses and domains, but with the volume of traffic that goes through an affected network, it may be difficult to pinpoint the exact attack vector. Using an IP WHOIS database to look up the contact details of a netblock owner can speed up an investigation. Law enforcement bodies can use the IP block ownership details as a starting point to identify, locate, and prosecute cybercriminals.

Beefing Up Cybersecurity

In 2016, researchers discovered that cybercriminals used more than 4 million IP addresses routed by Verizon. They stole the telco's unused IP blocks. However, since they need an extensive network to route IP addresses that won't arouse security personnel's suspicion, they chose Verizon. The telco unknowingly gave the cybercriminals a means to spread spam and other mayhem without worrying about being blocked.

Among the suspected spamming IP ranges routed by Verizon were:

```
14.4.0.0/15     PUBNETPLUS (Korea)
14.6.0.0/15     PUBNETPLUS (Korea)
42.128.0.0/12   North Star Information Hi.tech Ltd. Co. (China)
42.160.0.0/13   North Star Information Hi.tech Ltd. Co. (China)
42.168.0.0/13   North Star Information Hi.tech Ltd. Co. (China)
43.250.64.0/22  Infolink Communications (China)
103.41.180.0/22 Infolink Communications (Hong Kong)
116.129.0.0/16  New Guoxin Telecom Corporation (China)
116.132.0.0/15  New Guoxin Telecom Corporation (China)
116.136.0.0/15  New Guoxin Telecom Corporation (China)
116.138.0.0/15  New Guoxin Telecom Corporation (China)
116.140.0.0/15  New Guoxin Telecom Corporation (China)
116.142.0.0/15  New Guoxin Telecom Corporation (China)
116.148.0.0/15  New Guoxin Telecom Corporation (China)
116.150.0.0/16  New Guoxin Telecom Corporation (China)
116.152.0.0/15  New Guoxin Telecom Corporation (China)
116.156.0.0/14  New Guoxin Telecom Corporation (China)
116.160.0.0/14  New Guoxin Telecom Corporation (China)
116.164.0.0/14  New Guoxin Telecom Corporation (China)
116.168.0.0/15  New Guoxin Telecom Corporation (China)
116.179.0.0/16  New Guoxin Telecom Corporation (China)
116.184.0.0/13  New Guoxin Telecom Corporation (China)
120.46.0.0/15   CITIC Networks Management Co.,Ltd. (China)
120.48.0.0/15   CITIC Networks Management Co.,Ltd. (China)
155.40.0.0/16   Information Access Center (United States)
```

Source: Spamhaus?

Notice that most of the IP ranges are under the jurisdiction of APNIC. You can use that bit of information to strengthen your cybersecurity posture. For instance, you can feed the netblock details from the IP WHOIS database to your existing security solutions so they can monitor and block these indicators of compromise (IoCs) if necessary.

Expanding Your Network

Apart from protecting against and preventing cybercrime, IP netblock ownership information can also help organizations that wish to expand their networks. If, for instance, you are looking to buy

netblocks, you can download the IP Netblock WHOIS Database to check which blocks are available for purchase.

Enhancing Digital Rights Management (DRM)

Owners and distributors of digital media can better protect their copyright when they use IP netblock details to filter access to their materials. For example, a movie that only U.S. and European viewers should see can be made inaccessible to users from Asia and other regions. Feeding the APNIC IP netblocks information to filter out subscribers from the Asia Pacific region from authorized users is one way to do that.

Regardless of the reason why you want to trace APNIC block owners, what's most important is that you know it is possible. IP Netblocks WHOIS Database is, however, not limited to APNIC blocks alone as it also contains IP ranges from African Network Information Centre (AFRINIC) and other regional Internet registries (RIRs).