Recon With AI

BY:- BHUWAN PATIDAR

INTRODUCTION

There are lot of things available for recon in market (websites, application , cloud..) and all are good. but when it comes to best I will always suggest you to do manual recon because it gives you more results and understanding of your target. In this we will be looking at how I found best method for recon using Chatbots.

WHY CHATBOTS ?

During my recon on target lets say **X ,** I was searching for Origin IP and ASN regarding to X using Shodan, censys and Other tools but NO LUCK!!!! . Because it was behind Cloudflare.

Tried :-

1. **using ping got IP and CDN provider. (IP -> provider)**

2. **Searched and looked for leads with IP and Domain Name**
   Shodan -> Record Not Found
   Censys -> 4 Cloudflare IP with 403.
   (obviously there is nothing because they all belong to Cloudflare)

3. **Used tools but -> No Luck**

Now suddenly I got an idea why not to try AI for recon , as I have windows I tried to look for **X** on Copilot and results was amazing. as it was Australian Company.

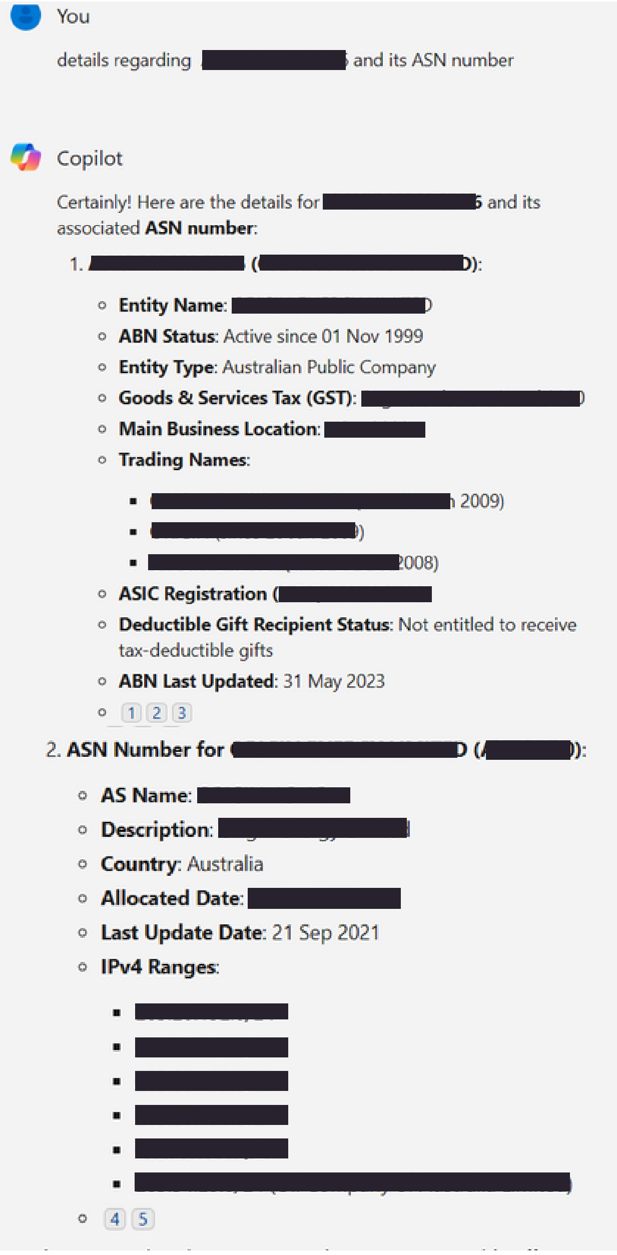
Achieved:-

1. **ABN Number**
2. **ACN Number**
3. **ASN Number**
4. **Peer ASN Number**
5. **IP-Range**
6. **Other Details of Company.**

HOW I DID 😊

I have used this trick on two most popular AI Chatbots ChatGPT and Copilot , where ChatGPT fails to provide expected results, it could be because my wrong Query. and Copilot rocks by giving all Answers .

1. Go to Copilot and search -> which organization owns $domain
2. Now go and check WHOIS data. if you found field with any number like Registrant ID etc.
3.details regarding $Registrant_ID and ASN Number



You

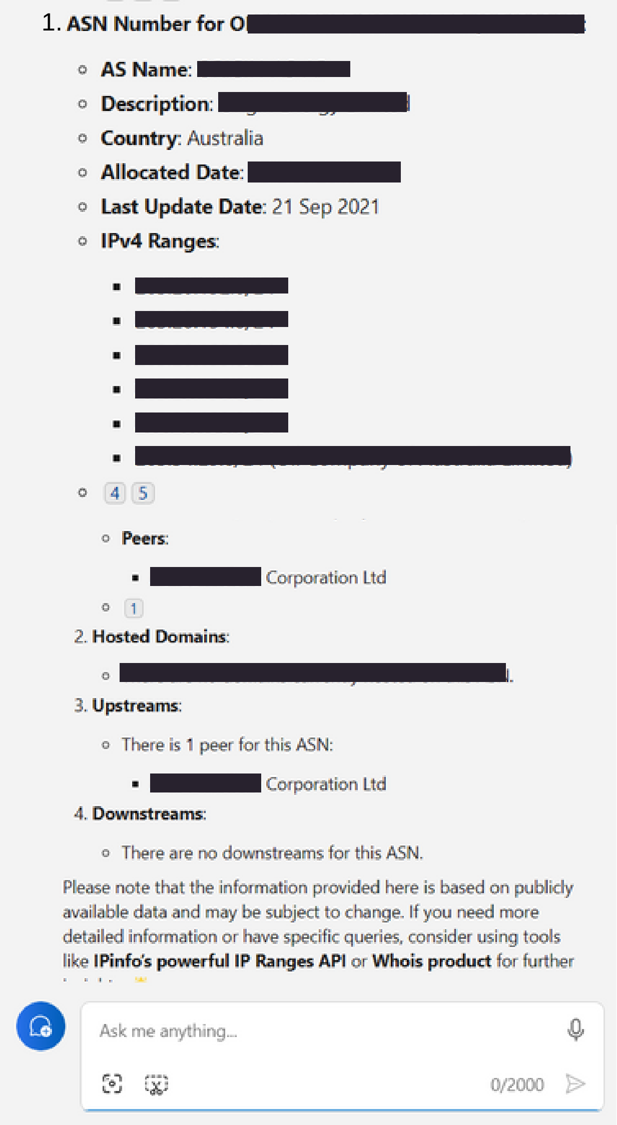
details regarding [redacted] and its ASN number

Copilot

Certainly! Here are the details for [redacted] and its associated **ASN number**:

1. **[redacted] ([redacted]):**
   - **Entity Name**: [redacted]
   - **ABN Status**: Active since 01 Nov 1999
   - **Entity Type**: Australian Public Company
   - **Goods & Services Tax (GST)**: [redacted]
   - **Main Business Location**: [redacted]
   - **Trading Names**:
     - [redacted] 2009)
     - [redacted]
     - [redacted]008)
   - **ASIC Registration** ([redacted]
   - **Deductible Gift Recipient Status**: Not entitled to receive tax-deductible gifts
   - **ABN Last Updated**: 31 May 2023
   - 1 2 3
2. **ASN Number for [redacted] ([redacted]):**
   - **AS Name**: [redacted]
   - **Description**: [redacted]
   - **Country**: Australia
   - **Allocated Date**: [redacted]
   - **Last Update Date**: 21 Sep 2021
   - **IPv4 Ranges**:
     - [redacted]
     - [redacted]
     - [redacted]
     - [redacted]
     - [redacted]
     - [redacted]
   - 4 5

4. search for -> Hosts Related to $ASN_NUMBER



1. **ASN Number for O**[redacted]
   - **AS Name**: [redacted]
   - **Description**: [redacted]
   - **Country**: Australia
   - **Allocated Date**: [redacted]
   - **Last Update Date**: 21 Sep 2021
   - **IPv4 Ranges**:
     - [redacted]
     - [redacted]
     - [redacted]
     - [redacted]
     - [redacted]
     - [redacted]
   - 4 5
     - **Peers**:
       - [redacted] Corporation Ltd
     - 1
   2. **Hosted Domains**:
      - [redacted]
   3. **Upstreams**:
      - There is 1 peer for this ASN:
        - [redacted] Corporation Ltd
   4. **Downstreams**:
      - There are no downstreams for this ASN.

Please note that the information provided here is based on publicly available data and may be subject to change. If you need more detailed information or have specific queries, consider using tools like **IPinfo's powerful IP Ranges API** or **Whois product** for further

- Peering Means
  - This statement implies that an organization (represented by the given ASN) has established a peering relationship with another organization (represented by ASN2).
  - The two ASNs are directly connected and exchange traffic without intermediaries.