

# Astrill VPN and DPRK Remote Worker Fraud

 [spur.us/astrill-vpn-and-remote-worker-fraud/](https://spur.us/astrill-vpn-and-remote-worker-fraud/)

Spur Engineering

December 19, 2024



## Astrill VPN Infrastructure

In our ongoing efforts to help organizations protect against fraud and abuse, we're excited to announce the free release of a comprehensive list of IP addresses associated with the VPN service known as Astrill VPN.

These ~2,400 IP address, active as of December 19th 2024, can be downloaded here:

<https://storage.googleapis.com/spur-astrill-vpn/ips.txt>

## Further Context

Recently, various intelligence and threat analysis teams have identified a concerning trend: North Korean state actors are infiltrating companies and organizations around the world in an attempt to facilitate the clandestine transfer of funds to support North Korea's state apparatus. Specifically, these actors have favored the use of Astrill VPN to obscure their digital footprints while applying for remote positions.

Much has been written about this topic. You can find more information at the following links:

<https://cloud.google.com/blog/topics/threat-intelligence/mitigating-dprk-it-worker-threat>

<https://unit42.paloaltonetworks.com/north-korean-it-workers>

<https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us>

While it's been several months since these articles were published, we continue to see reports from our customers of fraudulent remote worker campaigns originating from Astrill VPN IP addresses.

## **Spur's Mission**

---

At Spur, we are committed to providing the best, most relevant and up-to-date data on anonymizing services, including VPNs and residential proxies.

By sharing this data, we're hoping to help organizations enhance their security posture specifically against this particular threat from the DPRK.