SPUR

# IP INTELLIGENCE FEED

## Understand global attack networks

Anonymous infrastructure used by attackers has evolved. Static malware and botnets play a minor role in today's cybercrime complex. Attackers have gone to the "cloud"- leveraging large commercial anonymization networks as a service. With millions of clean, rotating proxies to route malicious traffic at their disposal, traditional defenses just won't cut it.

### The Problem (nobody knows about)

"Anonymization as a service" has skyrocketed. These quasi-legitimate services offer millions of nodes as proxies for arbitrary traffic. These networks are often constructed by bundling proxy features into legitimate software run by unwitting users. With such large and dynamic IP space available, these nodes are extremely difficult to detect. As a defender, how do you distinguish between legitimate users and a newly minted proxy? Since these proxy tools can be inside of legitimate software, how can administrators recognize when someone has proxy access to your internal network? Unfortunately, the realization that a device or IP was being used as a proxy is often too little, too late.

### The Solution

Spur has taken a new approach to combat these networks. We start by developing behavioral fingerprints for different anonymization services and their users. We then apply these fingerprints at scale across global internet activity. This approach provides a comprehensive snapshot of anonymization infrastructure and it's usage on the internet. The IP Intelligence feed includes all of this computation along with additional intelligence indexed by IP address.

### Our Data is Superior

Our approach to network discovery provides distinct advantages over our competition. First, we discover more types of anonymous infrastructure: residential proxies, privately operated VPNs, commercial VPNs, public proxies and peer-to-peer networks. Unlike other feeds, we label actual network exit points and not just entries. We also attribute the commercial service operator for that IP. Second, the IP Intelligence feed includes additional data on IP addresses not limited to

anonymization networks. This includes precise geolocation affinity, network ssids, and unique user count estimates. Technical client behaviors (such as usage of anonymous networks or peer-to-peer networks) are also provided. All of these components fit together to provide you with the context and information you need to protect your digital resources from modern anonymization techniques.

## Advantages to The Feed

The IP Intelligence feed has been designed to be used in and integrated into on-prem environments. It's structured JSON can be ingested directly into machine learning environments, application firewalls, event management engines or existing databases. Alternatively, the feed can be deployed as a local REST API using our public docker containers. Everything is organized by IP address.

## Common Use Cases

We are proud to help prevent:

- Denial of Inventory Attacks
- Fraudulent Purchases
- Fake Content, Reviews, and Spam
- Login Attacks and Masquerades
- Ad Fraud and Stuffing
- Application Level DOS

And support:

- Attribution and Tradecraft Discovery
- Risk Products and Security Operations

## Available Data

| | |
|---|---|
| PRECISION_GEO | The most significant geographic location affiliated with devices using an IP |
| SERVICES | The type of service being operated on this IP – such as commercial VPN operator or residential proxy network. We regularly track over 60 commercial VPN services and over 6 million residential proxy nodes. |
| USER_BEHAVIORS | Types of technical activities an IP engages in (e.g. VPN, proxy or peer-to-peer usage) |
| USER_COUNT | The estimated number of unique users behind an IP |
| ANON | Is this IP being used for anonymous activity |

## Contact Us

If you are looking for additional information, a sample, or are interested in purchasing our IP Intelligence feed please contact us at info@spur.us.