


Iranian APT Utilizing Commercial VPN Services

 spur.us/iranian-apt-utilizing-commercial-vpn-services/

Riley Kilmer

November 17, 2020

(Note: This post was migrated from the Spur website and was originally written on 11/17/2020)

TL;DR

APTs use commercial VPNs and proxies.

Knowing which service matters

Several weeks ago DHS/CISA issued an alert that Iranian actors were targeting US election websites. The actors scraped voter registration data, scanned for vulnerabilities, sent voter intimidation emails, and threw exploits.

The report makes a note that this actor uses VPN services for anonymity. Unfortunately, that isn't very specific. We (Spur) provide data to show *what* VPN services are being used. Threat actors, like everyone, have preferred tools, tactics, and techniques. Knowing these tactics makes for more effective defensive strategies.

I am going to walk through the list of IPs mentioned in the alert as Spur sees them with our data. Spoiler Alert: It's primarily Private Internet Access and Nord VPN, but there are outliers.

Analysis

Here is the full list of alert IP addresses we will look at:

102.129.239.185
104.206.13.27
109.202.111.236
143.244.38.60
154.16.93.125
156.146.54.90
185.191.207.169
185.191.207.52
185.77.248.17
194.127.172.98
194.35.233.83
195.181.170.244
198.147.23.147
198.16.66.139
212.102.45.3
212.102.45.58
217.138.211.249
217.146.82.207
31.168.98.73
37.120.204.156
37.235.103.85
37.235.98.64
45.139.49.228
5.160.253.50
5.253.204.74
64.44.81.68
70.32.5.96
70.32.6.20
70.32.6.8
70.32.6.97
70.32.6.98
77.243.191.21
84.17.45.218
89.187.182.106
89.187.182.111
89.34.98.114
89.44.201.211
92.223.89.73

First, I used the Spur [Context API](#) to enrich the IP addresses. Here is a sample result:

```
$ curl -H "token: $API_TOKEN" "https://api.spur.us/v1/context/185.191.207.52" | jq -r
'.{
  "anonymous": true,
  "as": {
    "number": 35758,
    "organization": "A.b Internet Solutions"
  },
  "assignment": {
    "exists": false
  },
  "deviceBehaviors": {
    "behaviors": [
      {
        "name": "TOR_PROXY_USER"
      }
    ],
    "exists": true
  },
  "devices": {
    "estimate": 100
  },
  "geoLite": {
    "country": "IL"
  },
  "geoPrecision": {
    "city": "Shiraz",
    "country": "IR",
    "exists": true,
    "hash": "tjm2e2",
    "point": {
      "latitude": 29.6219,
      "longitude": 52.5311,
      "radius": 500
    },
    "state": "Fars"
  },
  "infrastructure": "DATACENTER",
  "ip": "185.191.207.52",
  "proxiedTraffic": {
    "exists": true,
    "proxies": [
      {
        "name": "GEOSURF_PROXY",
        "type": "RESIDENTIAL"
      },
      {
        "name": "LUMINATI_PROXY",
        "type": "RESIDENTIAL"
      }
    ]
  },
  "similarIPs": {
```

```

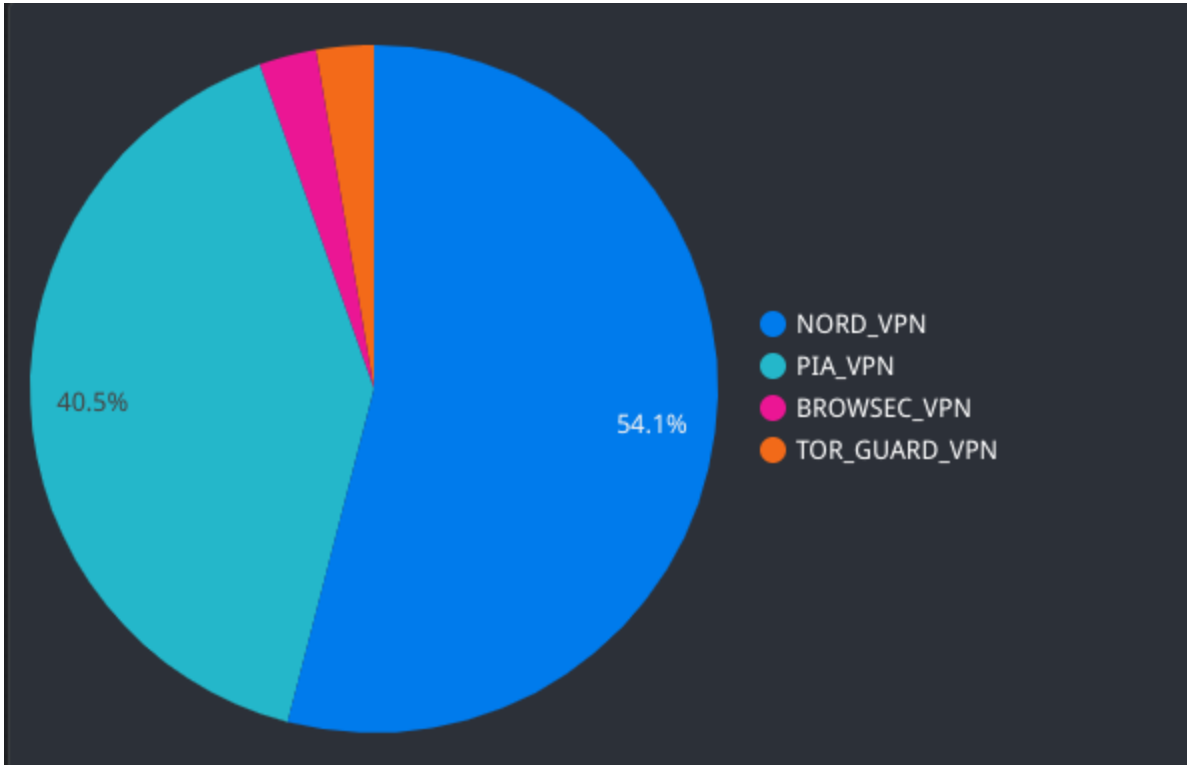
"exists": true,
"ips": [
  "185.191.207.164",
  "185.191.207.88",
  "185.191.207.137",
  "185.191.207.57",
  "31.168.98.73",
  "185.191.207.179",
  "87.239.255.38",
  "185.191.207.189",
  "185.191.207.12",
  "185.191.207.169",
  "185.191.207.36",
  "185.191.204.131",
  "185.191.207.132",
  "185.191.207.174",
  "87.239.255.105",
  "185.191.207.103",
  "80.179.42.30",
  "185.191.204.140",
  "185.191.206.4",
  "185.106.102.217",
  "185.106.102.204"
]
},
"vpnOperators": {
  "exists": true,
  "operators": [
    {
      "name": "NORD_VPN"
    }
  ]
},
"wifi": {
  "exists": false
}
}

```

Above, we can see that **185.191.207.52** is a Nord VPN exit. It averages 100 active users at any given time. This is busy, even for Nord. **185.191.207.52** proxies traffic for Luminati and Geosurf. Finally, the geo-precision field indicates heavy usage from Iran.

Services Used

A majority of the IPs belong to Nord VPN and PIA. There are two outliers: Browsec VPN and Tor Guard VPN. Is this another actor? Were these used for different activities?



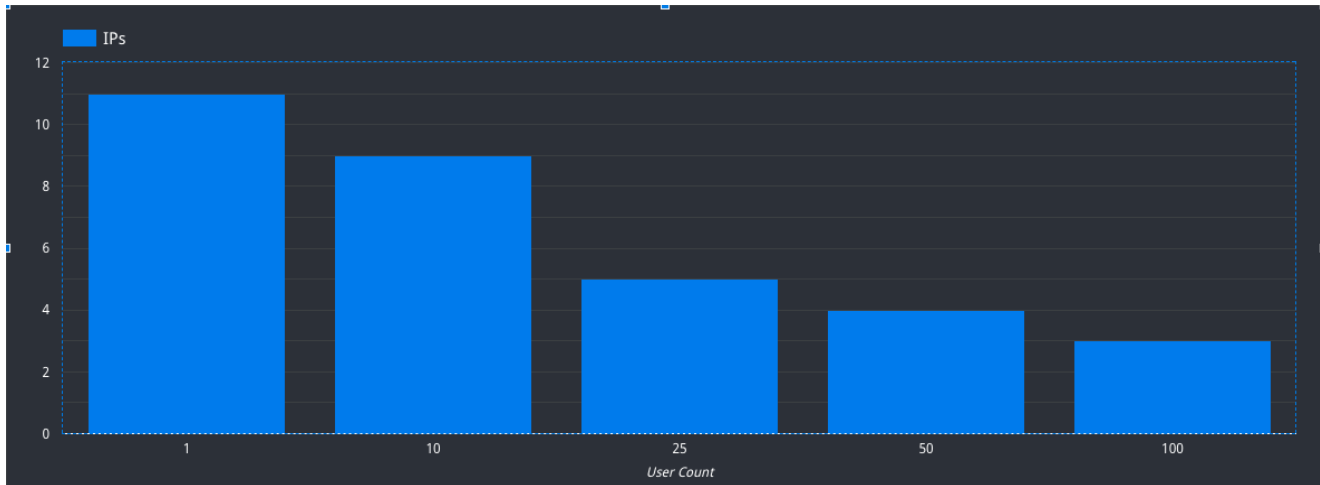
Exit Countries

The exit locations chosen (server location) are primarily in the US and Europe. It is possible the US was chosen to blend in on traditional server geo application or firewall rules.

- 16 US
- 5 GB
- 4 NL
- 4 IL
- 2 LU
- 2 BE
- 1 ZA
- 1 IR
- 1 FR
- 1 DE
- 1 CA

Usage Density

Usage density was varied across all of these IPs. Some serve a handful of clients, others are fairly large gateways. This insight can really help narrow down where analysts should focus attention.



The Non-VPN

Spur was not able to identify a VPN operating on **5.160.253.50**. This IP is especially interesting because it is a proxy in the Geosurf network. There are a few possibilities that could be worth exploring with more data. Is this their first hop IP? Is it possible that Geosurf is the actual common thread between all of these activities? Is this an anonymization or malware network Spur does not track?

Further Analysis

Some interesting questions could warrant further investigation:

1. This actor prefers Nord VPN and PIA. They also used Browsec VPN and Tor Guard VPN. How did activity differ between these?
2. The IPs have a wide range of activity volume. What threads can we pull from less active gateways?
3. Are we looking at the wrong thing? There is a high overlap with the Geo Surf residential proxy network. Perhaps this is the actual tradecraft for this actor.
4. Lots of threat intelligence services have picked up these IP addresses as high risk. Does that actually make sense for a shared commercial VPN?

Closing

Threat actors rely on VPN and proxy services. These services let them change IPs at will. Data on *what* service is being used enables more effective defense and analysis. Spur data gives technical attribution so that defenders and analysts make better decisions.

You can download the full context enriched data [here](#).

If you are interested in our data or services, please check us out at <https://spur.us>.