The Dark Side of the Router

By Dayton Dekam

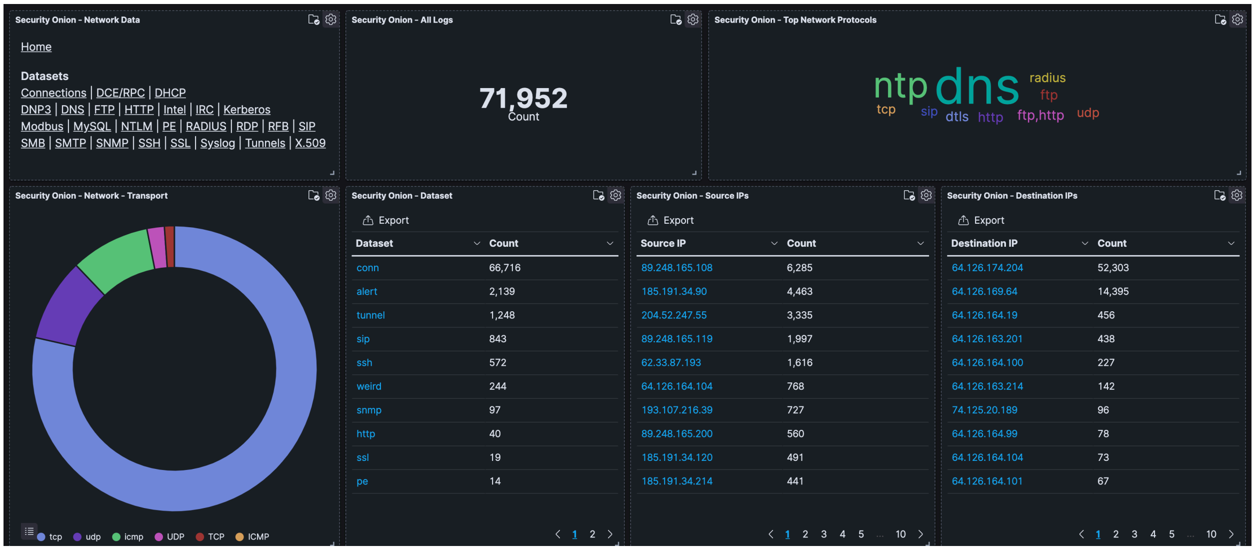
Most every household today is connected to the internet. Many of which have a dozen or more devices continually sending and receiving a waterfall of information almost continuously. Many of these devices are protected with anti-virus and frequent security updates to their operating system and various applications, and the security community has had a continual focus on keeping those endpoint devices secure from the many threats that endpoint devices face such as ransomware attacks and remote access trojans. However, besides the layers of kernel sandboxing and anti-virus, our endpoint devices might very well be the most protected by only a single device in the home, the router. Specifically, the NAT firewall on the home router may be one of the greatest layers of protection from hackers getting into our home devices. But how much malicious traffic really hits our router's NAT firewall? How often is the regular home router under attack from the outside world? This paper will explore those questions and dive into the very chaotic and spooky world of what's on the other side of that blinky box in our living room.

The Setup

To unveil this mystery, I first had to setup the network infrastructure to sniff all the packets on the internet facing interface of my router. To do this, I setup a hardware network tap device (SharkTap) between the cable connecting to my router and the one going through the wall out to the internet. Then I connected a third cable that went from the monitoring interface to a desktop computer running Security Onion 2. I knew this was a success when I saw the Cisco Discovery Protocol packets, which indicated I was monitoring the OSPF area upstream from my router.

Abnormal Traffic

I then let Security Onion do the work for me. It simply records the metadata of all traffic and their connection states going to and from my router, and the results were astonishing. After filtering out the normal traffic from my home by excluding connections initiated by my router's IP and the ISP's IP addresses, in just one week there are over 71,952 different instances of IP addresses sending packets to my router without me initiating a connection with them first. It's safe to say a lot of this traffic is not normal because traffic is not supposed to initiate connections to me. Connections should only be initiated from the home network. The dashboard I have at this point is below:


Security Onion - Network Data
Home
Datasets
Connections | DCE/RPC | DHCP
DNP3 | DNS | FTP | HTTP | Intel | IRC | Kerberos
Modbus | MySQL | NTLM | PE | RADIUS | RDP | RFB | SIP
SMB | SMTP | SNMP | SSH | SSL | Syslog | Tunnels | X.509
Security Onion - All Logs
Security Onion - Top Network Protocols
ntp
dns
radius
ftp
tcp
sip
dtls
http
ftp,http
udp
Security Onion - Network - Transport
tcp
udp
icmp
UDP
TCP
ICMP
Export
< 1 2 >
< 1 2 3 4 5 ... 10 >

71,952
Count

Security Onion - Dataset

Dataset	Count
conn	66,716
alert	2,139
tunnel	1,248
sip	843
ssh	572
weird	244
snmp	97
http	40
ssl	19
pe	14

Security Onion - Source IPs

Source IP	Count
89.248.165.108	6,285
185.191.34.90	4,463
204.52.247.55	3,335
89.248.165.119	1,997
62.33.87.193	1,616
64.126.164.104	768
193.107.216.39	727
89.248.165.200	560
185.191.34.120	491
185.191.34.214	441

Security Onion - Destination IPs

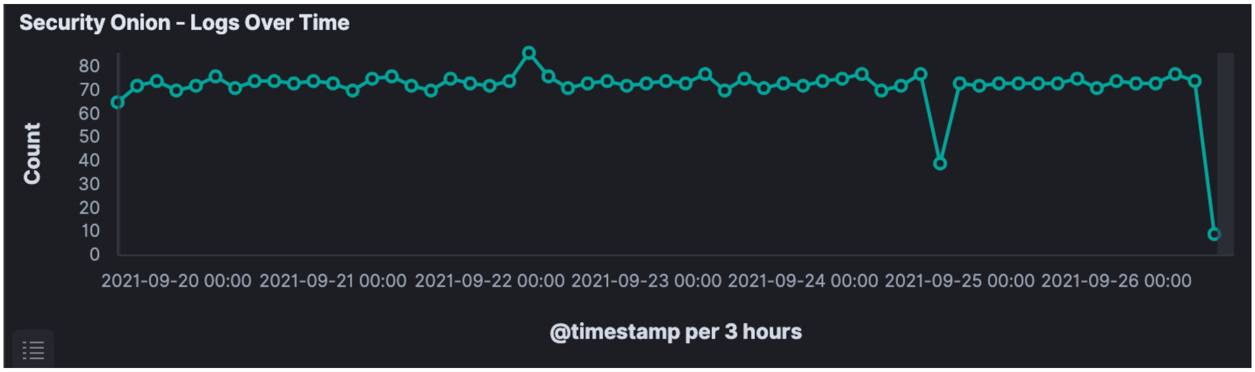
Destination IP	Count
64.126.174.204	52,303
64.126.169.64	14,395
64.126.164.19	456
64.126.163.201	438
64.126.164.100	227
64.126.163.214	142
74.125.20.189	96
64.126.164.99	78
64.126.164.104	73
64.126.164.101	67

As we can see, the majority of traffic from the outside world to my router is TCP along with an almost equally smaller portion of UDP and ICMP. The vast majority are connection requests, however for application layer protocols: sip, ssh, snmp, and http are the ones that stand out. The top suspect we have for a malicious IP address is 89.248.165.108 from the Netherlands, which in further detail appears to be TCP port scanning my IP on a range of higher port numbers from 48,000 and up. Running a WHOIS query on this IP, there was a tag of interest attributed to the registry that states the following:

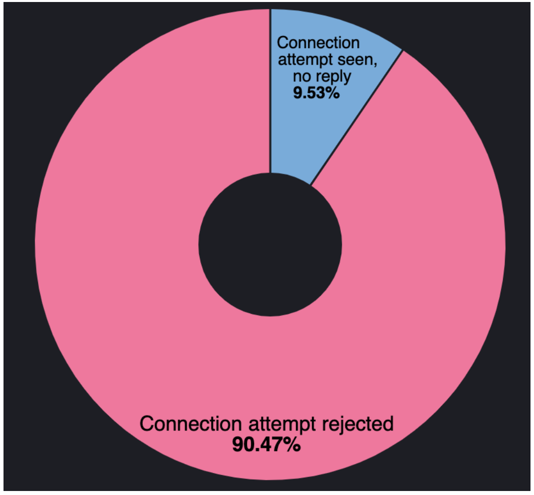
```
+------------------------------------------------
remarks:        | This net-block is not trying to hack you, we are only scanning
remarks:        | for LEGIT purposes ONLY. This scanning is done by multiple
remarks:        | security organizations.
remarks:        | Please use https://www.recyber.net/opt-out
remarks:        | to have your ip-address and/or netblock/as number white-listed
remarks:        | and excluded from this project.
remarks:        | If you have any further questions please contact admin@recyber.net
remarks:        +------------------------------------------------
```

Therefore, this IP not clearly an adversary, but more of a commercial information gathering botnet like Showden. This is interesting to find out the most common scanner that's hitting my router is not seeking to do harm, but research. However, I want to find the real bad actors and their TTPs, so I'll continue down the list.

The next most common IP attempting connections to my router is 185.191.34.90 out of Rostov-on-Don, Russia. Now things get interesting. The following graph shows the over four thousand connections this IP attempted to my router this week:



A WHOIS reveals this is reportedly owned by CY-STARCRECIUM. It has targeted only ports above 1000, which seems rather unusual since a network scanner normally prioritizes targeting service ports below 1000 rather than only probing higher number ports like this one. This is even more unusual when observing the frequency of this IP sending packets to my router. It's almost a completely consistent line aside from the two dips which is when I shut down security onion to update my computer. This warrants investigating more into the connection states to get a further idea of what they are trying to do. The following graph shows the connection states from this adversary.

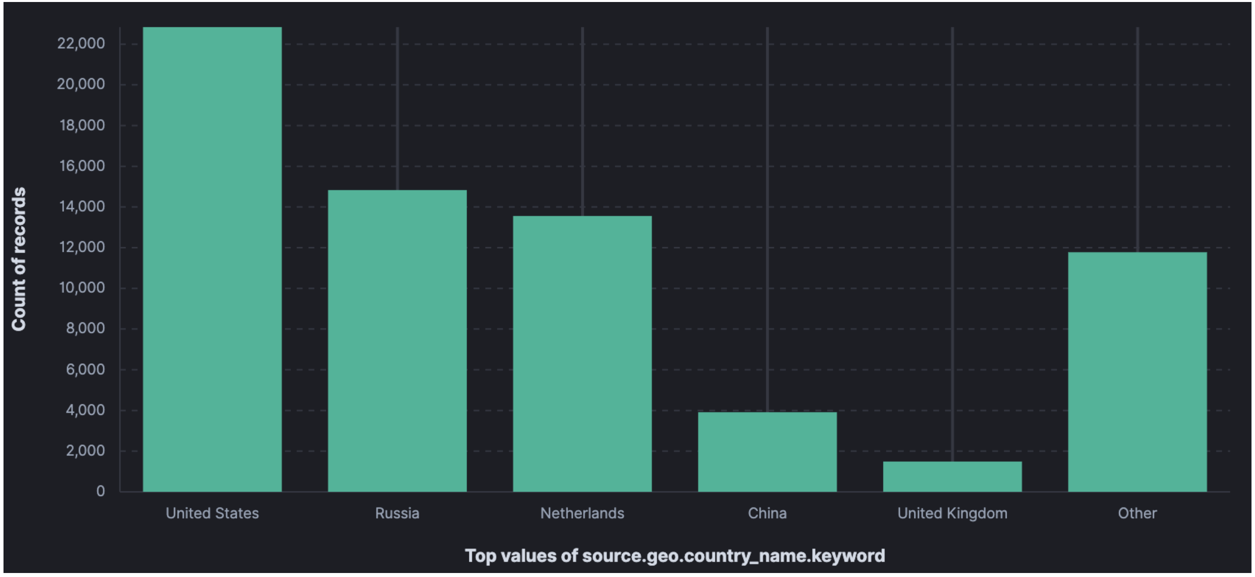


This graph is a bit of a relief at least. It shows that there were no connections actually established with this adversary, so they did not succeed. Almost 10% of the time my router did not respond at all, however over 90% of these my router sent an RST packet to the adversary. This is both good and bad. It's good that my router did not let the adversary connect on the requested port, but foolish to send an RST packet in response. This is because the adversary can map out which ports are closed and which ones are open based on the response. This leads to the chilling discovery that my router didn't hold silent that 9.53% of the time because of a firewall rule, but it did so because those ports are actually open and listening.

This router I rented from the ISP may very well not even have a firewall, and because of that, this adversary appears to have scanned my router and been able to infer which high number ports are listening, which with NAT, those listening high number ports are a portal into our home's electronics. This would make more sense of why this Russian based IP address doesn't even care about the service ports. They go straight for the gold by scanning high number ports where the router services are running and ports that are NATed to the internal network devices. To me this is very concerningly nefarious activity and I'll continue to monitor traffic from this IP further, and perhaps do a more deep packet inspection with a pcap.

The next IP, 204.52.247.55 is actually an IP address from the ISP, however I figured to mention it because all this traffic is purely ICMP error messages stating "Communication administratively filtered". This means there is a router ACL at that IP that is denying some traffic from my router to where it's going. This is likely the ISP doing a good job at stopping some traffic from getting to the bad guys. This might serve as some good news to the previous discovery where even though my router is responding with RST packets to adversaries, the ISP has a router upstream that is stopping some of the traffic to malicious locations so the bad guys might often not even be getting those RST packets. This might reveal this ISP takes the approach of centralizing their security rather than delivering it to the end points. In otherwords, instead of keeping a good firewall on all the routers, they just let the routers be responsive to attackers, but try to stop that bad traffic at an upstream focal network node.

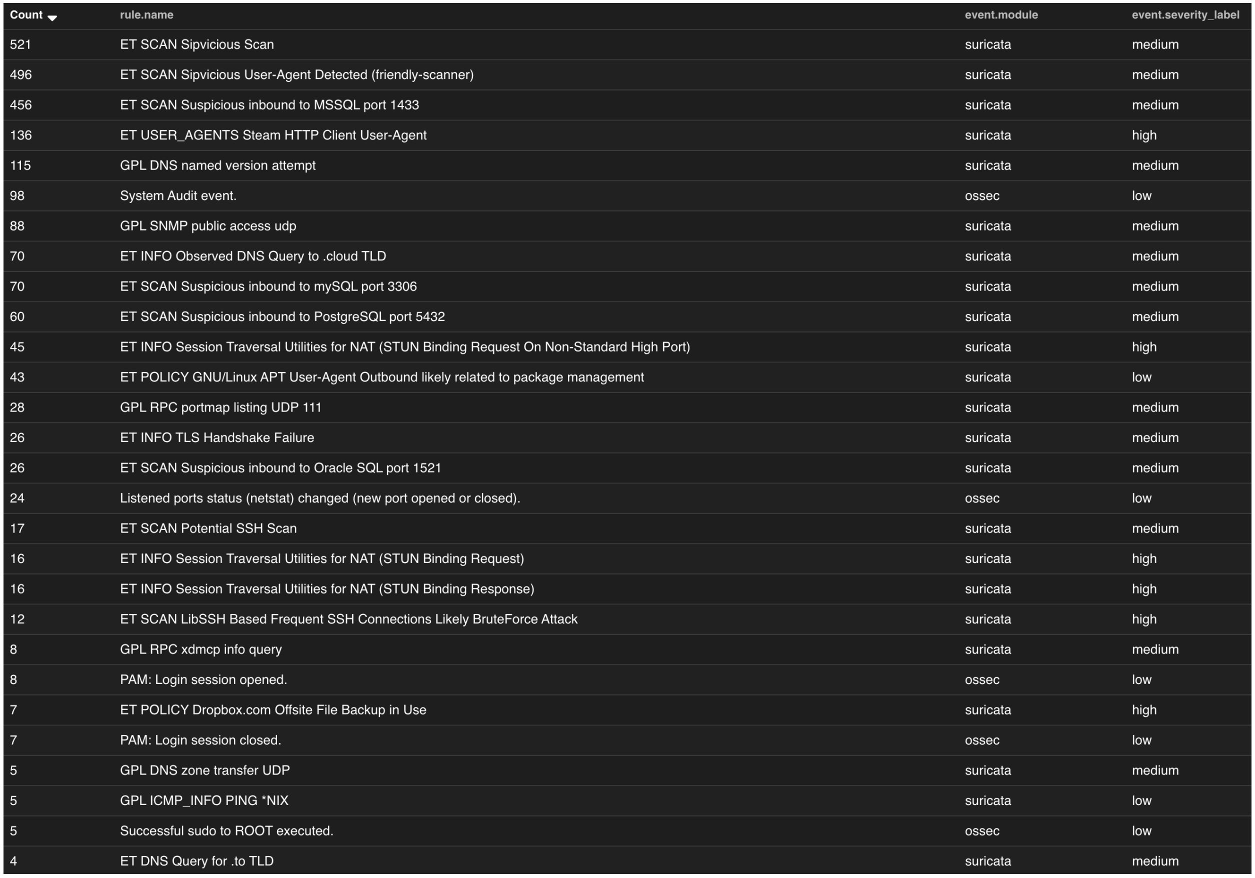
At this point a lot of the IP addresses from the US turn out to be owned by big tech companies such as Microsoft, Google, or Amazon, but further research might reveal those IP addresses to be either search engine spiders or cloud hosted virtual machines that attackers use. The following is a graph of countries that the majority of this traffic is from:



This portion of the study revealed that about 8% of the sessions to and from my router have been abnormal traffic. I hesitate to call this malicious traffic because all that is known so far about it is it's not normal traffic from devices on my network initiating a connection first. Most of which appear to be scanning/probing activity from mostly commercial bots and almost as commonly foreign IP addresses, especially Russia, where the motive isn't clear and could be malicious or intelligence related.

Aggressively Malicious Traffic

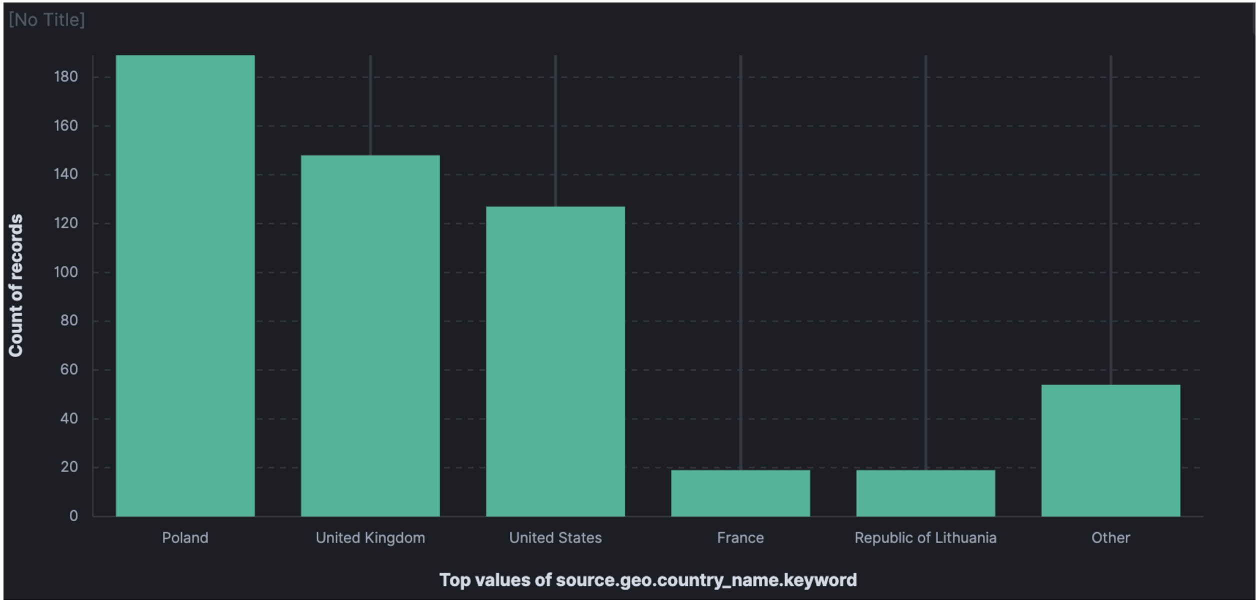
In this section we'll dive from our ten thousand foot view of the traffic to a much closer look where we single out only the malicious traffic that alerted in Security Onion. These are no longer just light scans or connection requests, but the less common traffic that is much more aggressive in nature. The following image contains the top alerts captured by Security Onion:



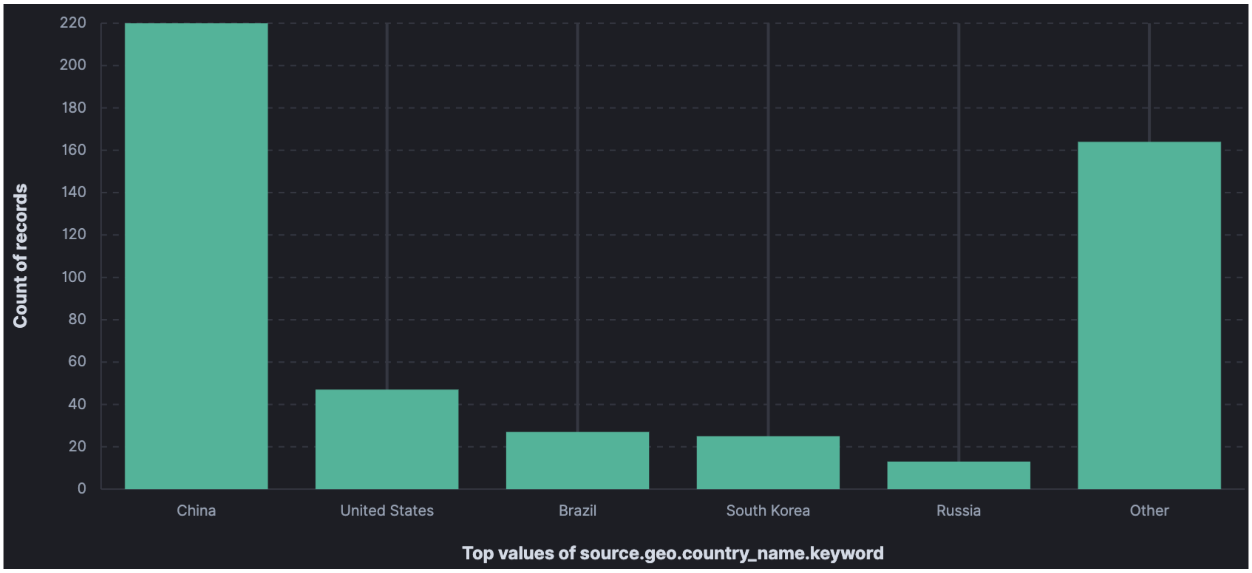
Count	rule.name	event.module	event.severity_label
521	ET SCAN Sipvicious Scan	suricata	medium
496	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)	suricata	medium
456	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium
136	ET USER_AGENTS Steam HTTP Client User-Agent	suricata	high
115	GPL DNS named version attempt	suricata	medium
98	System Audit event.	ossec	low
88	GPL SNMP public access udp	suricata	medium
70	ET INFO Observed DNS Query to .cloud TLD	suricata	medium
70	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium
60	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium
45	ET INFO Session Traversal Utilities for NAT (STUN Binding Request On Non-Standard High Port)	suricata	high
43	ET POLICY GNU/Linux APT User-Agent Outbound likely related to package management	suricata	low
28	GPL RPC portmap listing UDP 111	suricata	medium
26	ET INFO TLS Handshake Failure	suricata	medium
26	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium
24	Listened ports status (netstat) changed (new port opened or closed).	ossec	low
17	ET SCAN Potential SSH Scan	suricata	medium
16	ET INFO Session Traversal Utilities for NAT (STUN Binding Request)	suricata	high
16	ET INFO Session Traversal Utilities for NAT (STUN Binding Response)	suricata	high
12	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack	suricata	high
8	GPL RPC xdmcp info query	suricata	medium
8	PAM: Login session opened.	ossec	low
7	ET POLICY Dropbox.com Offsite File Backup in Use	suricata	high
7	PAM: Login session closed.	ossec	low
5	GPL DNS zone transfer UDP	suricata	medium
5	GPL ICMP_INFO PING *NIX	suricata	low
5	Successful sudo to ROOT executed.	ossec	low
4	ET DNS Query for .to TLD	suricata	medium

The top alerts are Sipvicious related which appears to be an aggressive scanning tool to discover and attack VoIP devices. The Steam HTTP Client User-Agent appears to be a false positive due to my desktop having the Steam application running and updating in the background. However, the other alerts show a common targeting on SQL such as mySQL and Microsoft SQL. Here are charts attributing the origins of the IP addresses of each alert:

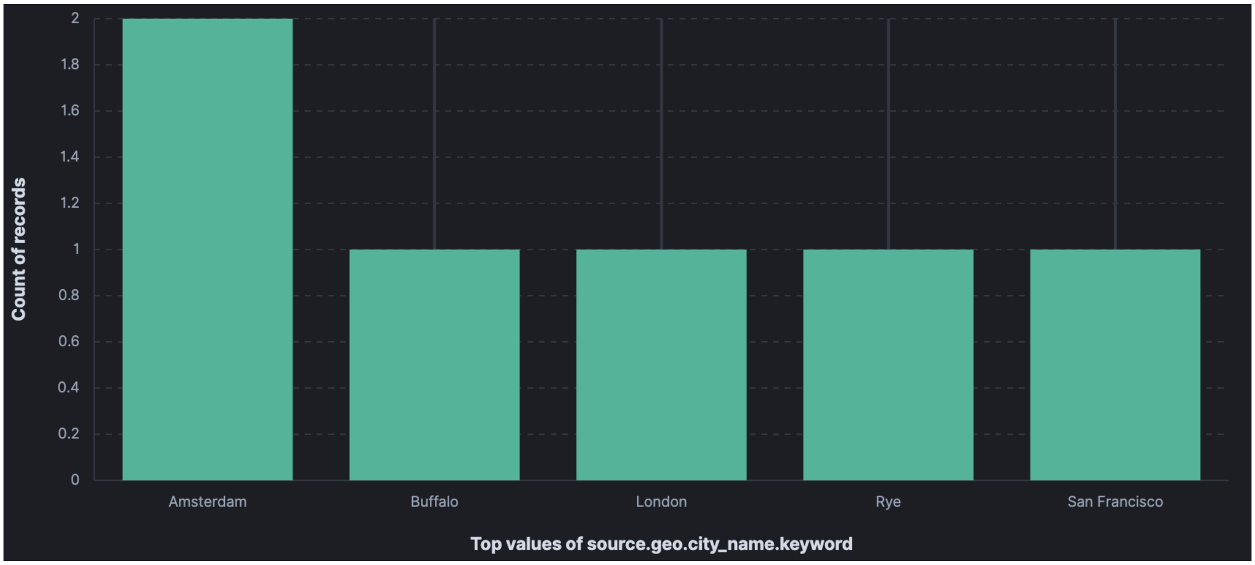
Sipvicious Scans:



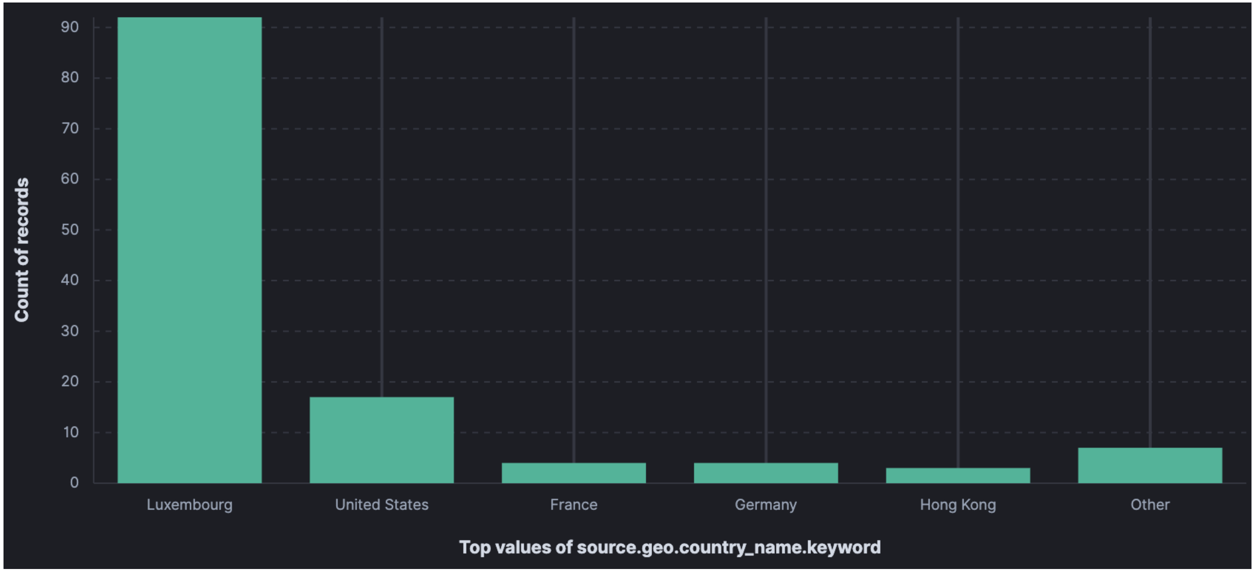
Port 1433 Microsoft SQL:



SNMP attacks:



DNS named version attempt:



Packets that don’t add up

One anomaly I found was there were over 409,000 packets that hit my router where neither the source or destination IP matched any of the DHCP IP addresses my router was issued during the week. A vast majority of them were IP addresses within the subnet of my ISP, however they just were not my router’s. The less than 5% of the others were very odd since they were IP addresses from out of this country. This might be due to errors in the routing tables of the OSPF areas that is accidentally spilling traffic to my router.

Conclusion

In conclusion this has been a first and surprising glimpse into the chaos on the other side of the home router and hopefully we can gain some appreciation for the NAT shielding our devices. It was surprising just how much traffic appears to be just commercial bots where the other large majority is originating outside the United States and appears to be more malicious. I will continue to dive deeper and perform deep packet inspection with Wireshark to gain a more clear idea of what these adversaries are trying to do and what payloads some of the more aggressive exploits are carrying. It’s important to note that all of these threats I have identified so far are defendable by simply configuring the router with a firewall or ACLs that drop any incoming packets that don’t have a connection established through the NAT on the router.