CEQUENCE SECURITY

Bulletproof Proxy Market Update

When a hot product hits the market, it is not uncommon to see multiple vendors follow the first market mover, selling the same, or very similar products. As noted in 2019 research done by Brian Krebs and in the CQ Prime Bulletproof Proxies research report, there were a few vendors marketing residential proxies (IP addresses) to the public. As the volume of stolen credentials continues to climb with weekly breaches, the market for criminal infrastructure to launch automated attacks is growing in parallel with new vendors emerging to market their network of residential proxies. Today its easy to find multiple Bulletproof Proxy vendors marketing their residential proxies to the public.

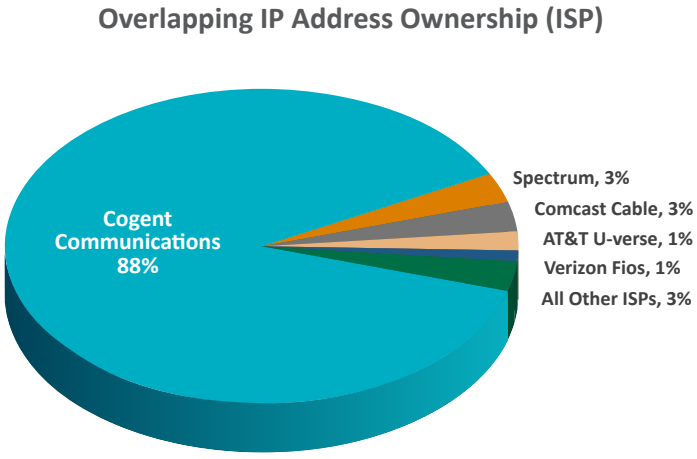
Common Bulletproof Proxy Uses

The first legitimate Bulletproof Proxy use case can be a simple desire to avoid geolocation-based censorship of internet content. People seeking to maintain anonymity browsing the web have every right to do so, and more importantly, these tools provide whistleblowers and suppressed individuals a means to communicate anonymously. Note that an individual only needs one proxy to maintain anonymity, not the millions that the vendors advertise. Another example would be organizations that want to test new features that may appear different to users in different countries, or with different types of IP addresses (residential vs mobile, etc.). Using these tools during the testing phase to validate is another potentially legitimate use case. In this case, the organization could take advantage of the higher number of proxies to simulate large user populations.

While these use cases are seemingly legitimate, one of the more common uses is for bad actors who want to execute cyberattacks while masking their identity and location. Account takeovers, fake account creation, scraping and API abuse are common automated attacks that take advantage of Bulletproof Proxies. To better understand the attack infrastructure our customers are faced with, the CQ Prime Threat Research team compared the "base product" of one of the new vendors to that of the older vendor used in our 2019 report.

No Honor Among Thieves

Comparing the two Bulletproof Proxy vendor offerings showed that roughly 34% of 22,000 North American IP addresses were for sale from both vendors. Essentially they are both selling the same exact same product. Both vendors had country, state and in some cases city breakdowns, allowing you to choose the geography that your traffic would originate from. Drilling into the source ISP for the overlapping IP addresses showed that 88% were owned by Cogent Communications, possibly as a carryover from their purchase of PSI Net assets. The remaining 12% were distributed across the remaining ISPs.



100% Malicious Usage

Analyzing customer attack data showed that 100% of the overlapping IP addresses were found to be generating account takeover traffic in both retail and financial services environments. A historical analysis of the overlapping IP addresses in those same customer environments showed they did not generate any legitimate traffic. Ever.

Retail Analysis

In retail environments, the attack traffic across the overlapping IP addresses was more heavily targeted at the web applications with the bulk of the attack traffic originating from Cogent Communications. Interestingly, the mobile API attack traffic was more evenly distributed across several ISPs with Verizon Fios most heavily used.

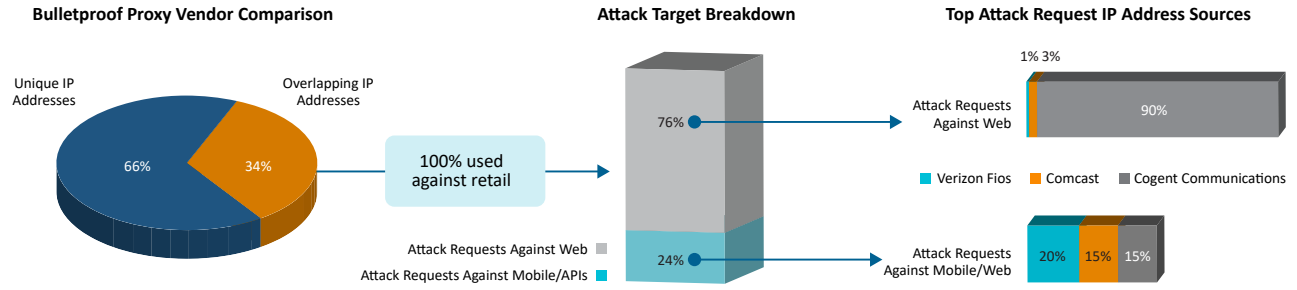


Image 2: Overlapping IP address analysis for retail customers.

Financial Services Analysis

Applying the same analysis to financial services customer data, the targets and the ISPs most commonly used were flipped. The mobile APIs were targeted almost exclusively with 88% of the attack traffic originating from IP addresses owned by Cogent Communications. Whereas the retail analysis showed attack traffic against web applications more evenly distributed across several ISPs, the financial services data shows 88% of the web attack originating from Cogent Communications.

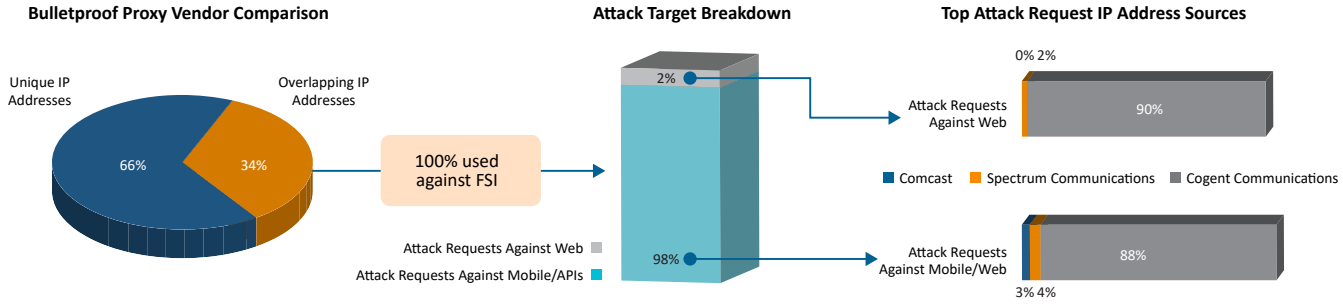


Image 3: Overlapping IP address analysis for financial services customers.

Building a Case for Outright Blocking

In most customer environments, there is a reluctance to blacklist large blocks of residential IP addresses because there is always a possibility a legitimate customer is blocked, resulting in a false positive and an unhappy customer. In reality, what are the chances of a false positive occurring? When the data shows that the IP address is known to generate ONLY malicious traffic and has never generated any legitimate traffic, as mentioned earlier, the case for blocking becomes more powerful and the chance of a false positive are low.

In cases where the probability is relatively high, for example a retailer and a customer, both in the U.S., we observed less than 0.8% of the overlapping IPs EVER appearing in good traffic over a 4 month period that included the peak periods of Thanksgiving, Black Friday & Christmas. The highest potential false positive rate observed was a maximum of 4% of all the overlapping IP addresses EVER generating legitimate traffic over an entire year (2019). The traffic from these IPs represented a miniscule < 0.1% of all traffic from known Bulletproof Proxy vendor IPs.

While some of these false positive rates are still too high to be acceptable over a long period of time, we've found that during bot attacks, these IPs almost NEVER send any legitimate traffic. This is where learned models that can detect, and block these Bulletproof Proxy IPs while they are committing abuse is important, and then automatically allow them to "become good again".