

The Threat of Residential Proxies to Sanctions Compliance

 spur.us/the-threat-of-residential-proxies-to-sanctions-compliance/

Spur Engineering

November 20, 2024

Key Takeaways

- Recently implemented sanctions by the United States and Western allies have been effective in limiting the financial activities of criminal organizations and nation state actors
- These malicious groups are becoming increasingly innovative in attempts to bypass regulatory restrictions to continue funding their activities
- The use of “residential proxies,” allowing entities in high-risk jurisdictions to temporarily borrow the IP address of an innocent victim’s phone or computer in another country is on the rise
- Existing IP quality score detection systems have a multi-month feedback loop requiring human investigations or chargebacks to resolve before the malicious activity they identify can be addressed
- Criminal use of residential proxies, and the shortcomings of traditional Geo IP based controls, is introducing additional BSA/AML risk for Financial Institutions
- Monocle (by Spur.us) takes a different approach, implementing advanced network telemetry and proactive monitoring to detect the technical methods of proxy activity. This provides your fraud, financial crime risk management, and cybersecurity teams with instantly actionable information to make sound decisions, allowing you to protect your organization and demonstrate a robust compliance program to regulators.
- Monocle detects/blocks online criminal traffic while authenticating legitimate digital customer sessions to avoid customer friction.

Understanding Residential Proxies

Residential proxies have long been used for illicit activity on the internet, including web scraping, scalping tickets to your favorite concerts, pushing spam to forums and social media, new account fraud and account takeovers. It involves hijacking what otherwise is legitimate infrastructure, allowing bad actors to mask their actual IP addresses with those associated with genuine customers your business would otherwise welcome.

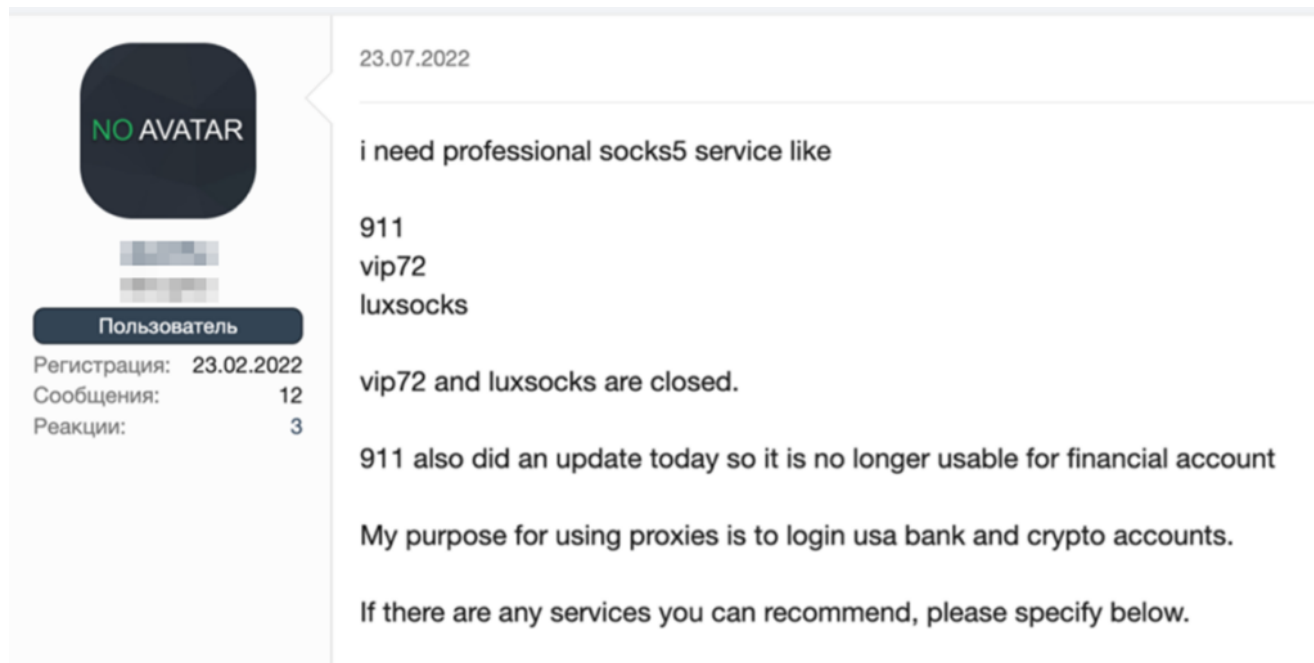
“Residential proxies” are so named because they utilize IP addresses that an Internet Service Provider has assigned to a household, as opposed to a business or datacenter. This makes them appear more legitimate and allows them to evade detection by legacy

geolocation and fraud services or IP quality score providers like [MaxMind](#) or [Transunion](#) (formerly Neustar).

Where Do Residential Proxies Come From?

[Residential proxies](#) are unique from other proxy offerings in several ways. Instead of a proxy company operating a server in a datacenter with access to thousands of IP addresses, they are based on software running on an individual phone or desktop computer. This software is either embedded into a [third-party application](#) such as a game or free mobile app (with the app provider getting paid for allowing the proxy company to access the mobile device), or the result of a malware infection with the hacker getting paid for allowing the proxy company to access their fleet of compromised devices. In some cases, the programs offer users free services such as VPNs or cash rewards for installing the proxy software; however, complicit users often do not understand the full scope of the (in many cases, illicit) activity they are facilitating.

Common Abuses of Proxies in Banking and Financial Services



The screenshot shows a forum post from a user profile. The profile has a dark blue header with 'NO AVATAR' in green. Below the header, the user's name 'Пользователь' is displayed in a dark blue box. To the right of the name, the registration date '23.07.2022' is shown. Below the name, the user's statistics are listed: 'Регистрация: 23.02.2022', 'Сообщения: 12', and 'Реакции: 3'. The main content of the post is a text message that reads: 'i need professional socks5 service like 911 vip72 luxsocks vip72 and luxsocks are closed. 911 also did an update today so it is no longer usable for financial account My purpose for using proxies is to login usa bank and crypto accounts. If there are any services you can recommend, please specify below.'

Residential proxies largely are used for gray-market purposes and cybercriminal activity. While gray-market activity may only violate various terms-of-service agreements, many proxy service providers will turn a blind eye to [much more nefarious](#) (and illegal) use-cases, including those involving banking and financial services.

One commonly seen fraud example is [Account Take Over](#) (ATO), where a malicious actor will pair stolen credentials with a residential proxy service before compromising an account and cashing out. Another well documented fraud example is new account fraud, where a

malicious actor will leverage BOTs and residential proxies to apply for new accounts with stolen and synthetic identities at scale.

Almost all residential proxy providers allow their customers to select proxies based on geographic regions, with targeting as specific as the city level. This feature enables criminal actors to effectively defeat existing fraud detection techniques such as flagging logins or transactions when the originating IP address is far away from their home or the location of their last login.

While residential proxies continue to be a key enabler of fraud losses on financial institutions and customer losses for scam victims, there is growing concern of the role residential proxies may be playing in recent headline grabbing BSA/AML regulatory news, including failures to prevent sanctions and OFAC violations. As previously highlighted, residential proxies allow for effective spoofing of geographic location, which in turn allows entities from sanctioned or high-risk jurisdictions to appear to originate within the United States (or other countries) for the purpose of account creation, conducting transactions, and facilitating the movement of funds.

Because proxies allow a single individual to operate under multiple online identities, they can be used to manage online accounts and structure transactions in a way that obfuscates who they really are and where they are really physically located. This introduces additional complexity for teams responsible for financial crime detection and management. No longer can financial institutions rely on traditional Know Your Customer controls and financial transaction based strategies and rule engines.

Financial institutions are having to build strategies on technical indicators like residential proxies to better detect and report on illicit activities spanning the FinCEN's US Government-wide Financial Crime Priority list. This is true for money laundering, sanctions, export violations, cybercrime, human and narco trafficking. It is also essential to mitigate cybercrime proceeds going to fund terrorist activities.

Regulators offer little mercy for financial institutions that facilitate sanctions evasion, even when unintentional.

Strategies for Effective Compliance

Navigating the regulatory compliance landscape is already a monumental challenge further complicated by residential proxies, VPNs, VDI providers, and other IP address obfuscation techniques. By implementing strong detections for each of these methods you can reduce the time to detection and mitigation for potential issues and reduce the workload of your security and compliance teams.

It is, however, notoriously tricky to detect this type of activity because both the bad actors and the anonymization service providers that facilitate them are constantly working diligently to remain undetected.

Existing Solutions

Many organizations have engrained legacy providers of geolocation data that are now attempting to pivot into labeling VPNs and other types of anonymization infrastructure; however, the workflows of these providers are focused on infrequent batch updates using data primarily sourced from public databases and feedback reports from their own customers. While this type of data is effective at stopping abuse from prolific low-effort sources, it is ineffective in combating more advanced and fast-moving sanctions-evasion activity.

Monocle by Spur

Real-time detection powered by Monocle takes a completely different approach. Using a simple and easy-to-deploy JavaScript tag or Mobile SDK, you can effectively tap into Spur's extensive historical detections database, continuous threat actor infrastructure scanning, as well as real-time network-fingerprinting techniques.

This game changing solution allows you to move beyond simply checking an IP address and instead interrogates the entire network flow and technical indicators using Spur's proprietary collection of detection techniques.

Are you ready to take the next step in enabling your compliance and security teams to address threats in real time? [Schedule a demo today.](#)