Digital Fraud Wiki

FRAUD DEFENSES

Crowdsourced Abuse Reporting
Device Fingerprinting
Email Reputation Service
IP Reputation Service
SR 11-7 Compliance
Supervised Machine Learning
Two-Factor Authentication (2FA)
Unsupervised Machine Learning

FRAUD TACTICS

Bot Attacks
Call Center Scams
Device Emulators
GPS Spoofing
P2P VPN Networks
Phishing Attacks
SIM Swap Fraud
URL Shortener Spam
Web Scraping

FRAUD TYPES

App Install Fraud
Application Fraud
Bust-Out Fraud

P2P VPN Networks

What is a P2P VPN Service?

A virtual private network (VPN) allows users to send and receive data, typically encrypted, across public or shared networks. The data is sent as though the device were connected directly to the private network. When a device is actively using a VPN, any application the device connects to sees the IP address provided by the VPN service instead of the real IP address of the device.

Traditional VPN services allow users to select from a list of specific IPs that the service maintains in various locations for a fee. However, peer-to-peer virtual private network (P2P VPN) services provide a new and often free form of VPN where a user can leverage the IP address of any other user in the network, and other users in the network can do the same.

What Should Companies Know About P2P VPN Services?

Fraudsters use P2P VPN services for location spoofing as well as spoofing and cycling through IP addresses, most of which are residential. Fraudsters can cycle through residential IP addresses so quickly that blacklists cannot keep up- our research shows that 65% of the overall IP addresses generated by fraudsters are used for seven days or less. On the other hand, traditional VPN networks are easy to blacklist, because the number of IPs available to users is

Loan Stacking

Synthetic Identity Theft

relatively low, and the IP addresses themselves don't change that frequently. Also, the IP addresses managed by traditional VPN networks are generally inside of public cloud services IP ranges.

P2P VPN networks are a highly effective way for fraudsters to evade IP reputation scoring services because IP reputation services reference blacklists as part of an IP address risk evaluation. P2P VPN networks also allow fraudsters to mimic authentic residential IP traffic such as hopping from IP to IP—behavior that would typically indicate a trustworthy user. Since P2P VPN networks allow fraudsters to access any of the IPs of real users, and because these users have residential IPs, it is nearly impossible to blacklist these IPs.

P2P VPN services provide fraudsters access to exponentially more IP addresses than traditional VPN services. P2P VPN networks are difficult to detect because of the volume, rapid cycling, and nature of the IPs available. Companies cannot rely on blacklists, IP reputation services, or traditional fraud prevention systems to detect and prevent modern fraud of this kind. Reliance on these approaches is ineffective due to the increasingly sophisticated tools and techniques bad actors use to commit fraud. More sophisticated systems are needed if organizations want to surface malicious activities quickly and accurately.

Prevent Sophisticated Fraud with DataVisor

The rise of fraudulent activity related to P2P VPN services offers a cautionary tale about emerging technologies. Organizations must always remember that fraudsters have equal access to the cutting-edge, and every time a beneficial and innovative new tool, technique, or technology is introduced and adopted, it is safe to assume it will be in use by fraudsters as well. Fortunately, unsupervised machine learning (UML) has emerged as a uniquely beneficial tool in the battle against modern digital fraud. When put to use by sophisticated fraud management solutions such as DataVisor's dCube, high-performing fraud models can do what reactive, legacy detection systems cannot, which is to identify burgeoning attacks-in-progress by the components of their digital footprints. Modern fraudsters are exceedingly adept at impersonating legitimacy, they operate at massive scale, and they are able to coordinate and manipulate high volumes of synthetic and fraudulent accounts. AI-powered detection systems are the only way to correlate the cross-account patterns hidden below veneers of seeming legitimacy.

Additional References

Webinar: DataVisor Webinar – The Sophistication Spectrum of Fraud

Source: VPN services: The ultimate guide to protecting your data on the internet, ZDNet

Source: Internet Protocol Version 6: IPv6 for Consumers, Federal Communications Commission