Digital Fraud Wiki

IP Reputation Service

What is an IP Reputation Service?

An IP reputation service provides a reputation score for an individual IP address that can be used by organizations as a signal in a fraud risk scoring system. IP reputation services became a popular solution for risk scoring because they not only signal that an IP address hosts malicious content but also that it exhibits automated bot behavior. Before the advent of IP reputation services, organizations relied primarily on solutions that linked the universal resource locator (URL) to malicious content such as spam, phishing emails, and malware. But URL-based solutions were not effective because they were slow in identifying attacks and fraudsters found ways to circumvent them. IP reputation services are now facing similar issues, as fraudsters leverage new tools and technologies to avoid detection.

What Should Companies Know About IP Reputation Services?

IP reputation services are limited when it comes to assessing the risk of an IP address because these services typically assess risk based on the history of the IP—whether the IP address has exhibited malicious activity in the past and if there are any changes since the last time the IP address was seen by the service.

Loan Stacking

Synthetic Identity Theft

Most IP addresses generated by fraudsters have virtually no history because fraudsters use tools such as cloud infrastructure and residential virtual private networks (VPNs) to mass-create anonymized IP addresses in a short period of time. The use of these tools by fraudsters diminishes the effectiveness of IP reputation services because the tools also allow fraudsters to spoof IP addresses and run bots that mimic authentic human behavior.

Residential VPNs are especially problematic for IP reputation services because they offer cheap residential IP addresses that allow fraudsters to mimic authentic residential IP traffic such as hopping from IP to IP—behavior that would typically indicate a trustworthy user. Fraudsters can also cycle through residential IP addresses so quickly that blacklists cannot keep up. IP reputation services reference blacklists as part of an IP address risk evaluation. Overall, our research found that 65% of the IP addresses generated by fraudsters are used for seven days or less. As fraudsters become increasingly adept at mimicking trustworthy user behavior, the effectiveness of IP reputation scoring systems will continue to deteriorate.

Another limitation of IP reputation services involves the sheer number of IP addresses that will need to be monitored, evaluated, and assigned a risk score as the number of available IP addresses increases from a little under 4.3 billion to approximately 340 ***undecillion*** under the rollout of Internet Protocol version 6 (IPv6). With so many IP addresses becoming available soon, it will be increasingly difficult for IP reputation services to monitor IP threat activity effectively.

Organizations must be prepared for high-scale malicious attacks involving staggering numbers of IP addresses. IP reputation services are not an adequate solution for the depth and scale of modern fraud. Organizations need a solution that assesses risk based on a wide range of signals and links among users and transactions.

Detect and Prevent Malicious Activity with DataVisor

Given the combined ease of mass-creating anonymized IP addresses in a short period of time, and the massive increase in available IP addresses, IP reputation services are no longer an effective fraud prevention mechanism. The only viable approach is to replace them with comprehensive, AI-powered solutions that can detect as rapidly as fraudsters act. The ability to correlate seemingly independent actions that are in fact part of a coordinated attack strategy is critical to detecting and preventing modern fraud, and it is

only through holistic analysis and contextual detection that malicious activity can be exposed while still in a pre-launch stage—before damage occurs.

Additional References

Webinar: DataVisor Webinar – Dumb & Dumber vs. Oceans 11 The Sophistication Spectrum of Fraud

Source: What is the total amount of public IPv4 addresses?, Stack Overflow

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

Source: Host IP reputation, Google Patents

Source: Neustar IP Reputation, Neustar

Source: minFraud riskScore, MaxMind