Digital Fraud Wiki

Bot Attacks

What is a Bot?

A bot is a software application that is programmed to perform repetitive, automated tasks over the internet. Thanks to bots, fraudsters can automate many of the tasks necessary to commit various forms of online fraud. Fraudsters today can initiate massive bot attacks to commit nearly any type of online fraud in a matter of minutes.

What Should Companies Know About Bot Attacks?

Bad actors use bots to accelerate the speed and scale at which they commit acts of fraud, and to cleverly disguise fraudulent activities. Also, fraudsters have intensified their attacks by turning to a new and more advanced type of bot called an advanced persistent bot (APB). APBs are capable of multiple obfuscation techniques including realistically emulating human behavior, dynamically rotating IPs, and distributing fraud attacks across thousands of IP addresses. APBs allow fraudsters to disguise coordinated fraudulent activities as authentic-looking user transactions and behavior.

No company conducting business online is immune to bot attacks. Here are a few examples of how bots are used for fraud:

- Online Marketplace Fraud – In the past, fraudsters would test which stolen credit card numbers were valid and active by

Loan Stacking

Synthetic Identity Theft

manually making small online purchases. Thanks to bots, the process for testing stolen credit card numbers can be entirely automated. Now fraudsters can test thousands of stolen credit card numbers quickly and easily. Fraudsters also use bots to commit product listing fraud on a grand scale. The bots are used to auto-generate massive numbers of fake product reviews from templates. The fake product reviews are used to boost the visibility of fake product listings on online marketplaces.

- E-Gift Card Theft – Not that long ago, fraudsters had to physically go to retail stores to write down gift card numbers before they could attempt to steal the balances. However, most fraudsters today use botnets to execute blunt force attacks on e-gift card websites. A botnet is a network of devices where each device is running one or multiple bots.

- Application Fraud – Fraudsters use bots to initiate massive application fraud attacks against financial institutions. Traditionally, fraudsters would complete credit applications individually and offline. However, many institutions now offer online lending services. Fraudsters use bots to automatically create hundreds, often thousands, of credit applications all at once through digital channels. Fraudsters also use bots to emulate the behavior of legitimate borrowers which makes the fraudulent credit accounts hard to detect.

A Holistic and Contextual Approach is Key

No matter the type of fraud, an online account created and maintained by a bot will likely appear legitimate when analyzed in isolation. Sophisticated bots such as APBs obfuscate fraudulent transactions and realistically emulate the activities of real users. To fight sophisticated fraud attacks, organizations must take a holistic and contextual approach to fraud detection. When analyzed as a whole and in context, bot-powered accounts reveal subtle patterns that can be used to defuse coordinated fraud attacks proactively.

Defuse Bot-Powered Fraud Attacks with DataVisor

With bots becoming increasingly omnipresent across the fraud landscape, organizations are now facing an entirely new scale of fraud. Bot-powered attacks often massive in size. Plus, they are challenging to detect, and extremely difficult to prevent, because the hallmarks of bot attacks can change very rapidly. To defeat bot attacks, organizations must have the means to meet scale with

scale. DataVisor's advanced fraud management solutions detect even the largest, most complex, most cleverly disguised attacks. Unrivaled domain expertise informs every feature of products like dCube—proprietary unsupervised machine learning algorithms adapt in real-time; massively scalable detection engines correlate behavior across users and accounts, and advanced feature engineering and data management capabilities make it possible to put up defenses against rapidly-evolving attacks.

Additional References

Solution: Bot Attacks

Solution: Application Fraud

Blog Post: Bot attacks, and one airline's battle to defeat them

Blog Post: Emerging Fraud in Marketplaces: How Product Listing Fraud is Gaining Traction

Source: Distil Networks' Sixth Annual Bad Bot Report Finds Bad Bot Arms Race Rages On, GlobeNewswire

Source: GiftGhostBot Attacks Ecommerce Gift Card Systems Across Major Online Retailers, Distil Networks