HUMAN

CDN and WAF solutions protect against simple bot fraud, but is it enough?

BotGuard for Applications
Case Study

1. An online banking provider initially opted to protect its consumers from account takeover attacks by adding the bot mitigation feature offered by its CDN/WAF provider.

2. HUMAN BotGuard for Applications revealed that 14% of the customer's total invalid traffic was made up of sophisticated bots impersonating humans, and this sophisticated invalid traffic (SIVT) was passing through the WAF/CDN's bot mitigation solution completely undetected.

3. The bank couldn't tolerate the risk to customers and the business associated with this level of detection inefficacy. They decided to augment protection from digital fraud and abuse including account takeover attacks with HUMAN BotGuard for Applications.

CHALLENGE:

Protecting Banking Customers from Fraud

A prominent online bank was relying on the bot mitigation solution packaged as an optional feature from its CDN/WAF provider. With online banking the top target of bot wielding cyber criminals due to high rewards, the customer couldn't sacrifice bot detection accuracy. The bank needed to effectively protect its customers and business from digital fraud and abuse including account takeover attacks, new account fraud, and sensitive data scraping.

SOLUTION:

BotGuard for Applications

HUMAN BotGuard for Applications was implemented across the online banking site to verify whether the existing WAF/CDN bot mitigation feature was sufficiently detecting all threats.

BotGuard's sophisticated Multilayered Detection Technology leveraging technical evidence, machine learning, threat intelligence, and continuous adaptation uncovered that 14% of invalid traffic was sophisticated bots and passing through the WAF/CDN's bot mitigation solution undetected. BotGuard revealed that most of the SIVT was originating from China and Pakistan, and while traffic from these countries was blocked by default, the traffic was bypassing the WAF/CDN's rule by hiding behind US and Canadian IP addresses.

BOT FRAUD PROFILE	
Daily Average Page Views	**75,000**
Daily Bot Traffic Rate	**14%**
Bot Traffic Originating Countries	**China, Pakistan**
Bot Traffic Originating ISP	25 Datacenter ISPs associated with cybercriminal operations

RESULTS:

Unstoppable Protection for Users from Digital Fraud and Abuse

In addition to implementing BotGuard for Applications via simple JavaScript (JS) tag integration, HUMAN's server to server (S2S) integration option enables passing additional business signals to BotGuard's Detection Engine, guaranteeing maximum detection accuracy and ultra-low false positives. The online banking provider was so reassured by the results of implementation via JS tag that they are moving forward with S2S API implementation to further customize the implementation and maximize results.

About Us

HUMAN is a cybersecurity company that protects enterprises from bot attacks to keep digital experiences human. We have the most advanced Human Verification Engine that protects applications, APIs and digital media from bot attacks, preventing losses and improving the digital experience for real humans. Today we verify the humanity of more than 10 trillion interactions per week for some of the largest companies and internet platforms. Protect your digital business with HUMAN. To Know Who's Real, www.humansecurity.com.