Un'fare' Advantage: Bots Tie up Airline Inventory

About Case Study

- One of the largest airlines in the world, operating over 5,000 daily flights to 300+ destinations worldwide
- Malicious bots assault its online reservation system, acting as faux buyers, to tie up tickets on certain flights, routes and classes of tickets.
- The airline can't distinguish between good bots that help it prosper in e-commerce and malicious ones that cost it revenue and profit

Who's the good guy? Leading airline overcomes malicious bots that avoid detection by mimicking user behavior

One of the largest airliners in the world loses revenue and profit when cyber-attacking bots are used to "scrape" its website for tickets, thereby locking up seats and forcing flights to take off only partially full. What technology did the airline rely on to distinguish the good guys from the bad?

Picture a service counter overcrowded with what appears to be legitimate customers. They only appear to be legitimate because none of them intends to make a purchase; rather their objective is to overwhelm the provider's resources and prompt other customers to go elsewhere. They succeed—with prospective buyers avoiding the gridlock and spending money with a different

provider. Addressing that kind of competitive tactic in the physical world might be simple enough. In the cyber world, the task is entirely different—and far more complex.

For a major US-based airline, this type of cyber-attack occurred with alarming frequency. Someone had created bad bots, programming them to "scrape" certain flights, routes and classes of tickets. With the bots acting as faux buyers—continuously creating but never completing reservations on those tickets—the airline was unable to sell the seats to real customers. In essence, the airline's inventory was held hostage, and a growing number of flights were taking off with empty seats that could have been sold.

To its credit, this airline had made significant investments in information security tools and resources. Even so, it found itself unable to distinguish between good bots that help it prosper in e-commerce and malicious ones that were costing it revenue and profit. That's because many of today's most severe security threats leverage bots and other traffic sources that can avoid detection by mimicking user behavior. This dynamically changes the source IP addresses or operating behind anonymous proxies and content delivery networks.

Device Fingerprinting to the Rescue

In the first half of 2015, this airline's executives made a strategic decision to invest in newer, more holistic technologies. One of the most important capabilities: device fingerprinting technology that could help the airline's systems distinguish good guy bots from the faux-buyer bots—and thwart the bad bots' attempts to lock up inventory. Device fingerprinting provides a more accurate means of identification than IP address and can be used to block malicious users and whitelist known legitimate users. It also can form the foundation of device reputational information for further security uses.

Similar to this airline, any business that conducts a high volume of online transactions can be a target of bots that exhaust application resources, illegitimately scrape sensitive information from websites and seek vulnerabilities by abusing application logic. To protect applications from advanced bots or even collective human threats, website operators need more advanced user and client identification that can detect and block illegitimate users.

To help combat this threat, companies have been ushering in technology that can track and precisely detect malicious end-user devices regardless of the source IP address. Device fingerprinting generally uses dozens of device characteristics in a unique way to identify and distinguish it from all others. Using this proprietary tracking, a company can generate device reputational profiles that include historical behavioral information to aid in the detection and mitigation of threats—from DDoS and intrusions to fraudsters.

Lessons Learned

As this airline discovered, accurate device-level identification enables effective protection from traffic that can elude security measures based on IP address. This includes malicious traffic coming through content delivery networks (CDNs) with whitelisted IPs and traffic using dynamic hosting configuration that results in a new IP address each time the device accesses the Internet. Device fingerprinting can also improve identification of malicious users accessing the Internet through Network Address Translation (NAT) devices that result in many devices sharing the same IP address, and anonymous proxy services that make it difficult to block IPs without potentially blocking legitimate users and devices.

Today, device fingerprinting technology has resolved the airline's challenge—and is helping other e-commerce organizations overcome similar threats from competitors and hackers.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.