DataDome

Security Alert: Bots Target NYC Restaurant Week

As NYC Restaurant Week approaches, restaurants are preparing to welcome diners to their establishments. However, the surge in demand for reservations also makes these booking platforms attractive targets for malicious bot attacks, including scalping, credential stuffing, and fraudulent account creation. These threats can disrupt operations, impact genuine customers, and lead to financial losses for both diners and restaurants.

Security Assessment of Table Booking Sites

DataDome conducted an assessment of various table booking websites to evaluate their vulnerability to bot attacks. The tests were conducted using an open-source bot framework without custom configuration, indicating that ***attackers using more advanced techniques could inflict even greater damage***.

Key Findings:

1. **100% of sites are vulnerable to fake account creation.**
   - Every site tested allowed bots to create an account.
   - Single Table Booking: Proof of concept confirmed that bots can book a table for two, far in the future, without triggering defenses.
   - Multiple Table Bookings: Bots were permitted to book multiple tables on the same day or within a short period, demonstrating the potential scalability of attacks.

2. **100% of sites have weak authentication measures, leaving them vulnerable to exploitation.**
   - Only 40% of websites used any bot detection solutions. None of these platforms prevented fake account creation or credential stuffing.
   - Only 20% of sites deployed a CAPTCHA.
   - Only 40% of sites sent validation emails or one-time passwords (OTPs) for registration or login.
   - 80% of the sites had no Multi-Factor Authentication (MFA).
   - Weak authentication measures left platforms vulnerable to exploitation through simple tactics like temporary email services and alias tricks**:**
     - Temporary email services, Gmail dot technique, and alias tricks were easily used to bypass registration checks.
     - Bots logged in without encountering substantial defenses.

Implications and Risks

- **Credential Stuffing:** Attackers can steal personal data, loyalty rewards, or hijack existing reservations by canceling and rebooking. Restaurants requiring deposits risk financial losses for legitimate customers.
- **Mass Account Creation:** Attackers can create and resell fake accounts, which may be leveraged in future attacks if the platforms implement stricter defenses.
- **Scalper Activity:** Attackers can book high-demand tables en masse, reselling reservations or holding them hostage.

Recommendations

To mitigate these risks, table booking platforms can take steps to enhance their security posture.

- **Advanced bot protection:** Transition from basic CAPTCHA systems to more sophisticated bot management solutions that provide real-time detection and mitigation of automated threats. This will help prevent bot attacks at every stage of the user journey.
- **Strengthen registration processes/** Enforce email validation or OTP verification during account creation and login, and deploy robust MFA to secure user accounts.
- **Enhance booking defenses:** Introduce behavioral analysis to detect and block abnormal booking patterns (e.g., rapid, repeated table bookings). Monitor for unusual activities, such as bulk bookings across multiple days.
- **Educate users.** Encourage users to enable security features (if available) and monitor their accounts for suspicious activities.

Conclusion

Bot attacks targeting restaurant booking platforms pose a significant threat, especially during high-demand periods like Restaurant Week. Our findings demonstrate the ease with which attackers can exploit these vulnerabilities, underscoring the urgent need for comprehensive bot mitigation strategies. By implementing advanced security measures, restaurants can safeguard their platforms, protect their patrons, and ensure a seamless dining experience for all.