radware

THE TOP AUTOMATED BOT THREATS TO APPLICATIONS AND HOW TO STOP THEM

"Bad" bots, which masquerade as humans and attack online businesses, now comprise 26% of total internet traffic. They evade conventional security technologies, threatening websites, mobile applications and even APIs. Often, these highly sophisticated and automated threats set their sights on web applications, using an array of tactics to pillage personal data, tie down online inventory and degrade application/website performance.

These attacks often go undetected by conventional mitigation strategies because bots have evolved from basic scripts to large-scale distributed bots with humanlike interaction capabilities to evade discovery. Staying ahead of this threat requires two things: a firm understanding of these malevolent robots and more sophisticated, advanced security capabilities to actively detect and mitigate them.

To address the former, the Open Web Application Project (OWASP) seeks to remedy these threats by maintaining a list of automated attacks that target web applications.[1] It serves as a starting point for security professionals seeking to ensure protection of web applications from the most virulent threats currently available to cybercriminals.

These threats can be grouped into six categories:

- Account Takeover
- Payment Data Abuse
- Web Scraping
- Denial of Inventory
- Skewed Marketing Analytics
- Denial of Service

Bot management solutions address the latter and now serve as a cornerstone of any application security strategy. The escalating intensity of bot traffic and the increasing severity of its overall impact mean that dedicated bot management solutions are crucial to ensuring business continuity and success.

This document provides an overview of these categories, symptoms by which to identify them and key technical capabilities that security professionals should consider when evaluating bot management solutions.

[1] https://www.owasp.org/index.php/OWASP_Automated_Threats_to_Web_Applications

ACCOUNT TAKEOVER

This category encompasses ways that bots are programmed to use false identities to obtain access to data or goods. Their methods for account takeover can vary. They can hijack existing accounts by cracking a password via Brute Force attacks or using known credentials that have been leaked via credential stuffing. Lastly, they can be programmed to create new accounts to carry out their nefarious intentions.

As its name suggests, this category encompasses an array of attacks focused on cracking credentials, tokens or verification codes/numbers with the goal of creating or cracking account access to data or products. Examples include account creation, token cracking and credential cracking/stuffing. Common symptoms of these include higher than average account creation rates or high numbers of failed token/account login attempts from the same user and/or IP address.

MITIGATION BEST PRACTICES:

Intent-based deep behavioral analysis (IDBA) is a critical next-generation capability to mitigate account takeovers executed by more advanced generation 3 and 4 bots. IDBA leverages the latest developments in deep learning and behavioral analysis to decode the true intention of bots. IDBA goes beyond analyzing mouse movements and keystrokes to detect humanlike bots, so “bad” bots can be parsed from legitimate traffic to ensure a seamless online experience for consumers.

IDBA is a major step forward in bot detection technology because it performs behavioral analysis at a higher level — abstraction of intent — unlike the commonly used, shallow interaction-based behavioral analysis. Account takeovers are an example of intent, while a “mouse pointer moving in a straight line” is an example of interaction. Capturing intent enables IDBA to provide significantly higher levels of accuracy to detect more advanced bots. In addition, device and browser fingerprinting capabilities are equally critical to discern the identity of end-user devices for bots that leverage evasion techniques such as changing IP addresses or operating behind anonymous proxies. Credential cracking (also known as a Brute Force attack) represents a simpler form of account takeover typically executed by legacy script-based bots. It can be mitigated by applying rate limiting on various collected parameters for login pages, authentication pages and API call authentication pages.

AVAILABILITY OF INVENTORY

This category of threats specializes in holding hostage the inventory of e-commerce sites, ticketing systems, airlines, etc. It accomplishes this by beginning the purchasing process without checking out and timely restarting the process whenever the time for closing elapses. Additional bots clear inventory instantaneously, so cybercriminals can resell goods. The result is direct financial loss.

Denial of inventory and scalping are two perfect examples. Denial of inventory means depleting goods or services without completing the purchase or committing to the transaction. Scalping, on the other hand, is focused on obtaining limited-availability items/services via “unfair” tactics. Scalping is typically characterized by peaks of traffic for certain goods while denial-of-inventory attempts usually result in increased stock held in baskets or reservations, elevated basket abandonment rates and a dramatic reduction in the payment step process.

MITIGATION BEST PRACTICES:

Mitigating denial of inventory is based on the type of bot performing the attack. Legacy generation 1 and 2 bots can be mitigated by applying custom rules to cart pages/APIs to block attempts to programmatically add products to carts. Stopping more advanced generation 3 and 4 bots will require the aforementioned IDBA. Workflow and visitor journey validation are critical for mitigating both of these threats while also ensuring minimal false positives.

WEB SCRAPING

Web scraping bots are designed to harvest and steal data. Everything from pricing information, website content, screen captures — and even files — are up for grabs.

Data scraping is a perfect example of web scraping. This attack type is a common practice in digital publishing or e-commerce sectors and is designed to collect application content and/or other data for use elsewhere. Unusual request activity for selected resources, duplicated content from multiple sources in search engine results and decreased search engine rankings are common symptoms associated with data scraping.

MITIGATION BEST PRACTICES:

Mitigation requires an integrated approach. Certain web application firewalls (WAFs) typically do well at mitigating common scraping attacks by leveraging device and browser fingerprinting. A dedicated bot management solution can accurately detect and mitigate more sophisticated bot activity with the detection of humanlike bots through the use of IDBA, which is also required to prevent data scraping by advanced bots that use more sophisticated evasion techniques. This provides the added benefit of improving the user experience by only applying certain mitigation practices, such as CAPTCHA, to mischievous bots and not to legitimate users.

PAYMENT DATA ABUSE

These bots conduct fraudulent activity against credit cards and other payment methods, either by guessing or abusing already known (usually stolen) payment details.

Carding and its close relative card cracking are common examples of this category of web application abuse. As their names suggest, both are designed to leverage credit card data. Carding attempts to validate stolen payment card data. Signs include elevated basket abandonment, reduced average basket price, a higher proportion of failed payment authorizations and the disproportionate use of the payment step.

Symptoms of card cracking are similar and also include elevated basket abandonment and a higher proportion of failed payment authorizations but can include increased chargebacks as well.

MITIGATION BEST PRACTICES:

Make sure that your organization can analyze anomalous behavior specific to payment gateways to detect and block carding attempts.

To block card cracking attempts, a bot management solution should be able to combine multiple streams of data, including mouse movements, keystrokes and URL traversal patterns to block bots from programmatically cracking payment cards.

SKEWED MARKETING ANALYTICS

Bots can interfere with business analytic systems and processes, which include digital advertising, affiliate programs and PPC, to eventually cause the victim to make incorrect decisions based on false reporting/data. Skewing, ad fraud and spamming are perfect examples of this category of application abuse, among others.

Skewing and ad fraud revolve around click abuse to alter web performance and advertising metrics and, as a result, revenue. Both are highlighted by decreases in clicks/impressions and conversions in addition to highly skewed metrics that fall well outside typical thresholds.

Spamming, on the other hand, is the act of posting fake and questionable information on forums.

MITIGATION BEST PRACTICES:

Machine learning is a cornerstone for mitigating these types of abuses. For skewing, apply domain-specific, machine learning techniques to identify anomalies in user behavior and block bots from affecting business KPIs. An enterprise-grade bot management solution can use JavaScript tags to collect hundreds of parameters to identify sophisticated bot patterns and prevent skewing in addition to assisting with estimating and filtering the nonhuman traffic present in paid and organic acquisition reports. To that end, make sure that any bot management solution can also integrate with analytics platforms such as Adobe and Google.

Mitigating these attacks has a clear impact on the bottom line. Organizations receive clean analytics to receive actionable insights, eliminate skewing of products and growth metrics and filter bots from traffic analytics to optimize marketing spending and drive revenue.

Spamming is best mitigated by leveraging time series-based machine learning to detect fraudulent form submissions and spam comments on online portals and forums.

DENIAL OF SERVICE

As a new version of a legacy attack vector, these bots target web/mobile applications and websites with the intention of making resources unavailable, thereby achieving denial of service (DoS). Ultimately, reduced website performance and service degradation are telltale signs of a DoS attack on a website or web application. Application unavailability or a sudden increase in user account lockouts is also a giveaway.

MITIGATION BEST PRACTICES:

Make sure that your bot management solution can accurately detect and restrict sudden spikes of automated activity on critical application resources to avert any attempt by scammers to exploit security vulnerabilities in business logic. Make sure that you partner with a bot management provider that leverages threat intelligence gathered from thousands of internet properties and applies device fingerprinting to detect attacks.

Finally, any bot management solution should be part of a layered integration with other DDoS mitigation systems. Bot management solutions are excellent at accurately detecting and parsing malicious bots from legitimate traffic, but ensuring service availability of your online services requires DDoS mitigation as well. An enterprise DDoS mitigation appliance will reside at the network perimeter and use its own behavioral-based mitigation capabilities to protect against known and unknown DDoS attack vectors. The bot management solution complements these capabilities by providing the DDoS appliance with real-time data feeds for comprehensive protection.

CONCLUSIONS

For organizations both large and small, securing the digital experience means securing your applications, online properties and mobile interfaces. The rise in malicious bot traffic and, more specifically, sophisticated bots that mimic human behavior necessitates the need for a dedicated bot management solution. Being able to distinguish and stop the wolf in sheep's clothing is critical to ensuring business continuity and success.

LEARN MORE ABOUT RADWARE BOT MANAGER.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.