radware

Guide

The Ultimate Guide To The OWASP 21 Top Automated Threats and Security Capabilities To Stop Them

TABLE OF CONTENTS

There are good bots that help online businesses improve search engine rankings and provide a better customer experience. Then there are malicious bots that have evolved their evasion techniques to the extent traditional security solutions such as web application firewall (WAF) and CAPTCHAs are rendered ineffective in detecting them.

From web scraping and bypassing CAPTCHA challenges to engaging in nefarious activities like spamming, account takeover, credential stuffing, sniping and carding, automated bots are the most preferred tool used by attackers, fraudsters, competitors and other adversaries. The actors behind these fraudulent activities keep improving the automated programs to create even more advanced persistent bots that can accurately mimic human behavior to evade detection when they attack.

The rise in automated bot attacks on web applications moved the Open Web Application Security Project (OWASP) to create the OWASP Top 21 Automated Threats To Web Applications. It's designed to allow organizations to better understand and respond to the increased threats from automated bots.

Based on the OWASP list, this guide provides an overview of each automated threat and mitigation capabilities that a dedicated bot management solution should provide to stop them.

TABLE OF CONTENTS

OAT-01: Carding

Carding is an automated form of payment fraud in which fraudsters test a bulk list of credit/debit card data against a merchant's payment processing system to verify the stolen card details. Such card details are stolen from different payment channels or other applications or purchased from dark web marketplaces. Hackers also apply card cracking (OWASP OAT-010) practices to obtain credit card details.

Mitigation

A general best practice is to outsource all aspects of payments to providers that are equipped with adequate facilities to address carding attacks. Additionally, increasing the minimum checkout value and IP blacklisting are tried-and-true best practices.

Bot mitigation solutions should adopt a different approach and should leverage deep user behavior and intent analysis to eliminate carding attacks.

OAT-02: Token Cracking

Token cracking is the process of gaining access to identification tokens, which are cryptographic keys that are generated by online services. Tokens are often sent to users via text message on their mobile devices.

Tokens may be used for multi-factor authentication (MFA), where an additional factor of authentication is required if the user wants to access data from an unknown device or location. This form of two-step verification is intended to prevent unauthorized access to sensitive data, but cybercriminals can gain access using brute force methods. This can result in identity theft and other types of fraud. If the token is compromised, the attacker gains complete control over the victim's account and can track all activity and change or delete information.

Mitigation

Security experts recommend multi-factor authentication (MFA) for users, leveraging two or more forms of identification rather than just one. Along with MFA, operators of websites and applications would be well advised to implement a bot mitigation solution to detect and prevent bots that use phishing techniques such as robocalls that purport to be security verification calls from the website or application. Such tactics dupe unsuspecting victims into providing their one-time passwords or security codes to the attacker.

OAT-03: Ad Fraud

Digital ad fraud refers to the deliberate act of misrepresenting or obfuscating ad engagement metrics. It is committed by fraudulent traffic (from bots as well as humans) that generates dummy impressions and adversely affects the click-through rate (CTR). The invalid activity from bots drains ad-serving resources and affects publishers' efforts to build a premium ad inventory. Non-human traffic also distorts site analytics and affects marketing campaigns. In addition, invalid traffic hurts a publisher's brand reputation, impacts ad verification reports, and harms quality scores. Currently, most security measures are ineffective in filtering human-like bot activity. Various types of ad fraud can include traffic sourcing, ghost sites, domain spoofing, ad stacking, pixel stuffing and ad injection.

Mitigation

Publishers should leverage a bot solution with intent analysis and pre-bid filtering alongside fingerprinting techniques and collective bot intelligence data to understand user intent and accurately filter sophisticated invalid traffic (SIVT) before ads are served to avert ad fraud in real-time. A bot solution greatly helps in monitoring and blocking synthetic traffic, allowing the publishers to assure their advertisers that the CTR statistics reflect genuine impressions.

Advertisers should have access to bot intelligent reporting that can accurately classify invalid traffic, including crawlers, traffic from known data centers, and SIVT, which can help in getting detailed insights on the quality of the impressions and clicks.

The bot management solution should also be serving CAPTCHAs, presenting JavaScript challenges or any other form of challenge-and-response high-risk score.

Responses to these challenges help build a closed-loop feedback system that dynamically improves machine-learning models and assist in minimizing false positives down to negligible values.

OAT-04: Fingerprinting

With fingerprinting, specific requests are sent to the application eliciting information to profile the application. This probing typically examines HTTP header names and values, session identifier names and formats, contents of error page messages, URL-path case sensitivity, URL-path patterns, file extensions and whether software-specific files and directories exist.

Fingerprinting is often reliant on information leakage, and this profiling may also reveal some network architecture/topology. The fingerprinting may be undertaken without any direct usage of the application, e.g., by querying a store of exposed application properties such as held in a search engine's index.

Symptoms can include single HTTP requests, often none, but possibly requests for a wide range of missing resources and requests for resources that are rarely requested.

Mitigation

Tried-and-true best practices include randomizing the content and URLs of payment submission pages and payment forms in addition to rate-limiting authorization attempts per session, user, IP address, device and fingerprint.

Bot mitigation solutions should leverage techniques that can detect and prevent fingerprinting attacks that are typically executed to probe for potential vulnerabilities that can be exploited to carry out harmful attacks.

OAT-05: Scalping

Scalping is an age-old practice that used to be carried out by scalpers and resellers buying event tickets and certain goods that were in high demand and later selling them for a considerable profit.

Today, scalping has mostly moved online, so scalpers now use sophisticated "all-in-one" bots that are sold online and programmed to regularly scan e-commerce, ticketing, and other websites and applications to find and quickly buy large quantities of desired products (such as certain brands of sneakers and gaming consoles) before regular consumers even get a chance to log in to make their purchases. The scalped products are then quickly resold through sites like eBay and other portals that serve the secondary market.

Scalper bots are deployed to regularly visit popular e-commerce portals at frequent intervals to scan for product "drops" — launches of highly anticipated products such as sneakers or gaming consoles, event tickets and other products in limited supply. The scalpers behind these bots first create user accounts at online stores under various identities, using different IP addresses, payment cards, and shipping addresses, and combinations thereof, to evade fraud detection systems.

Mitigation

Many e-commerce portals have implemented limits on the number of items that buyers can place in their shopping carts. Others now require in-person pickup of products from their stores or have introduced points of friction to slow down scalping activities (which can also irritate genuine shoppers). These can include requiring proof of identification, solving CAPTCHAs, issuing tokens that give priority to existing customers or those enrolled in loyalty programs, and so on. Unfortunately, none of these approaches are scalable for large e-commerce and ticketing portals, as scalpers usually find ways to defeat these mitigation practices.

Scalper bots are easily available to buy online, and some sophisticated bot developers even provide customer service and outsourced CAPTCHA-solving processes to enable their users to make the most out of them. If an enterprise tries to stop bots using traditional approaches such as blocking IP addresses or certain regions and data centers, scalper bot operators can easily resort to using hijacked residential devices and proxy IP addresses to slip under the radar of conventional defense systems.

A sophisticated bot management solution uses multiple approaches to curb the scalper problem. A combination of behavioral analysis and machine learning with device fingerprinting does a real-time analysis of the traffic to identify and block malicious bots. Bot vendors supporting challenge-response authentication like the crypto challenge "proof-of-work" can add onto the multilayered protection from automated programs.

OAT-06: Expediting

Expediting is the process of using speed to violate explicit or implicit assumptions about the application's normal use to achieve unfair individual gain, often associated with deceit and loss to some other party.

In contrast to OAT-016 skewing, which affects metrics, expediting is purely related to faster progression through a series of application processes. OAT-017 spamming is different from expediting, since the focus of spam is to add information and may not involve the concept of process progression.

A common symptom of expediting is uncharacteristically fast progress through multi-stage processes.

Mitigation

An organization can accurately identify and restrict automated usage via fingerprinting devices to block malicious bots. A sophisticated bot management solution can detect evasive tactics used by attackers to obfuscate their device fingerprints, and it leverages collective bot intelligence data and artificial intelligence to detect bots in real-time.

OAT-07: Credential Cracking

Also known as "brute forcing," credential cracking is a way to identify valid credentials by trying different values for usernames and passwords (usually from lists of breached account credentials that were made public by malicious parties and hackers). Hackers deploy bots to hack into customers' accounts using the brute force approach, dictionary attacks (inputting large numbers of words), and guessing attacks to identify valid login credentials. Brute force attack symptoms include a sudden increase in failed login attempts and high numbers of account hijacking complaints from customers.

Mitigation

Many approaches are used by online businesses to eliminate bot traffic and prevent account takeover attempts. The list includes time-worn practices such as limiting login attempts, a robust authentication process, IP blacklisting, configuring rules in a WAF, and CAPTCHAs.

Bot detection and mitigation solutions should leverage behavioral and intent analysis, machine learning, and device and browser fingerprinting to mitigate malicious bots attempting to execute credential cracking attacks to take over accounts. They should ideally also include dedicated machine learning to protect URLs and APIs, along with new-age crypto challenges to detect and block malicious bots.

OAT-08: Credential Stuffing

Credential stuffing exploits users' propensity to use the same username and password at multiple websites. Hackers use bots to test lists of credentials obtained as a result of data dumps of breached credentials (or purchased from the dark web) against a range of websites, in the hope that a victim has used the same combination of credentials on multiple sites.

Unlike credential cracking, credential stuffing doesn't involve brute force or guessing of any values; instead, mass login attempts are used to verify the stolen username and password pairs. Credential stuffing symptoms include consecutive login attempts with different credentials from the same HTTP client.

Mitigation

Several approaches are used by online businesses to eliminate bot traffic and prevent account takeover attempts. They include practices such as limiting login attempts, a robust authentication process, IP blacklisting, configuring rules in a WAF, and CAPTCHAs.

Bot detection and mitigation solutions should leverage non-intrusive API-based approaches to mitigate malicious bots attempting to execute credential stuffing attacks to take over accounts. They should ideally also include intent analysis techniques to catch bots.

Progressively increasing JavaScript challenges will help in curbing the attacks faster because they increase the resource usage for the malicious bots, forcing them to discontinue their attack.

OAT-09: CAPTCHA Defeat

While CAPTCHA is deployed to distinguish legitimate users from bots, threat actors use CAPTCHA-defeating bots to leverage automation to analyze and determine the answers to visual and/or aural CAPTCHA tests and related puzzles/challenges.

Common symptoms are high CAPTCHA-solving success rates on fraudulent accounts or suspiciously fast/fixed CAPTCHA solving times.

Mitigation

Organizations can consider monitoring and limiting the rate of card authorization attempts per session, user, IP address, device and fingerprint. Due to this, suspicious authorization attempts and malicious users are blocked as soon as they have reached a set number of failed attempts while testing different card numbers.

Identify and restrict automated usage by reputation methods. In particular, businesses can use geolocation and/or IP address block lists to prevent access to payment parts of the application.

Organizations can make use of bot solutions offering crypto challenge as a mitigation solution to identify and block the CAPTCHA-solving bots. With the crypto challenge "proof of work," there is no CAPTCHA presented to the user in this case, and with no CAPTCHA presented, it will be much harder for bots to try and solve it.

OAT-10: Card Cracking

Similar to carding (OAT-1), with card cracking, bots conduct fraudulent activity against credit cards and other payment methods, either by guessing or abusing already known (usually stolen) payment details. Card cracking is a common example of web application abuse and leverages credit card data. Card cracking attempts to validate stolen payment card data.

Symptoms of card cracking are elevated basket abandonment, reduced average basket price, higher proportion of failed payments, elevated basket abandonment, and a higher proportion of failed payment authorizations and include increased chargebacks.

Mitigation

Make sure that your organization can analyze anomalous behavior specific to payment gateways to detect and block card cracking attempts. Additionally, 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.

OAT-11: Scraping

Content scraping (also referred to as web scraping or data scraping) is lifting unique/original content from other websites and publishing it elsewhere. Content scrapers typically copy all content to pass it off as their own, including blogs, research, product reviews, financial information, etc.

Content scraping, on a basic level, can be accomplished by manual copy and paste. More sophisticated techniques involve bots that are used to crawl websites and copy thousands of pages within a matter of seconds.

Content scraping is a commonly practiced method by online publishing companies that rely on ad revenue to fuel their websites. Third-party scrapers crawl and copy high-quality, keyword-dense content from other websites. Additionally, bloggers and media publishers are usually targeted to steal content from their websites.

Mitigation

Ensure a bot mitigation solution provides intent analysis capabilities and applies semi-supervised machine learning techniques, device and browser fingerprinting, behavioral modeling, and dynamic Turing tests to block scraper bots.

API protection is also critical. Scrapers and competitors exploit vulnerable APIs with bots to steal sensitive data. Again, machine learning is critical, combined with proprietary models such as API flow control, authentication flow, intent-based behavioral analysis and invocation context to accurately detect and block bad API calls.

OAT-12: Cashing Out

Cashing out is a process of obtaining currency or higher-value merchandise via the application using stolen, previously validated payment cards or other account login credentials. Sometimes cashing out may be undertaken in conjunction with product return fraud.

Common symptoms include increased chargebacks, increased usage of interlinked accounts and an increased demand for higher-value goods or services.

Mitigation

The organization can consider limiting the number of transactions per user, IP address, session or device or can even consider increasing the verifications required at the checkout pages to demotivate fraudsters.

Apart from anomalous behavior or traffic detection and mitigation, using a bot management solution also has the advantage of collective intelligence – threat intelligence sharing among databases. Collective intelligence helps identify bot networks faster across geographies while registering any new attack patterns and sharing the same for the larger benefit.

OAT-13: Sniping

Sniping is a last-minute bid or offer for a particular good or service. It's made at the last possible opportunity, leaving insufficient time for another user to bid/offer.

Sniping can also be the automated exploitation of system latencies in the form of timing attacks. Careful timing and prompt action are necessary parts. It is most well-known as auction sniping, but the same threat event can be used in other types of applications. Sniping normally leads to some dis-benefit for other users, and sometimes that might be considered a form of denial of service.

Common symptoms are increasing complaints from users about being unable to obtain goods or services or some users having higher success rates than expected.

Mitigation

An intelligent way to identify and stop sniping bots is to monitor bypassing steps to fulfill the checkout/confirmation page. Monitoring bypasses and incomplete steps will give insight into any unusual trends and higher-than-normal success rates.

With a dedicated API machine-learning module along with intent analysis, a sophisticated bot management solution can identify any anomaly in the API flow and invocation context.

OAT-14: Vulnerability Scanning

Vulnerability scanning is scanning and crawling an application to identify weaknesses and possible vulnerabilities. It's a systemic enumeration and examination of identifiable, guessable and unknown content locations, paths, file names and parameters, in order to find weaknesses and points where a security vulnerability might exist. Vulnerability scanning includes both malicious scanning and friendly scanning by an authorized vulnerability scanning engine.

Symptoms include elevated occurrence of errors; extremely high application usage from a single IP address; a high ratio of GET/POST to HEAD requests for a user, session or IP address; and multiple misuse attempts against application entry points.

Mitigation

Along with monitoring authorization failures or failed authentications, organizations can also implement a limit on the number of input validation or authorization failures per user, session, IP address or device.

Implementing specialized vulnerability-scanning tools will help the organization in controlling and curbing these scans. Implementing a bot manager solution helps in evading attacks that are carried out by making use of these vulnerabilities.

OAT-15: 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

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 distributed denial of service (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 solution as well. The bot management solution complements these capabilities by providing the DDoS mitigation solution and/or WAF with real-time data feeds for comprehensive protection.

Bot management solutions also complement cloud DDoS mitigation systems and WAF with their behavioral and intent analysis to identify and block automated programs.

OAT-16: Skewing

Bots can interfere with business analytic systems and processes, which include digital advertising, affiliate programs and pay per click (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.

Mitigation

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 marketing analytics platforms.

OAT-17: Spamming

Spamming is the act of posting fake and questionable information on forums, comment sections, blogs, wiki webpages and public-facing webpages and content contribution platforms.

Mitigation

Per the aforementioned mitigation strategies for skewing, spamming is best mitigated by leveraging time series-based machine learning to detect fraudulent form submissions and spam comments on online portals and forums.

OAT-18: Footprinting

Footprinting is an online security threat that involves gathering information with the objective of learning as much as possible about the composition, configuration and security mechanisms of the application. Unlike scraping, footprinting is an enumeration of the application itself, rather than the data. Footprinting is used to identify all the URL paths, values, parameters and ad-process sequences. As the application is explored, additional paths will be identified, which in turn need to be examined.

Footprinting can also include brute forcing and dictionary attack techniques. Fuzzing may also be used to identify further application resources and capabilities.

Common symptoms can include an increase in system and application error codes, such as HTTP status codes 404 and 503, or user behavior that falls outside of typical user behavior.

Mitigation

Protecting URLs and important APIs becomes a priority for an organization; differentiating good calls from bad helps in quickly identifying and blocking malicious parties from taking advantage of any vulnerabilities. Along with the intent analysis are dedicated ML modules for APIs such as flow control, invocation context, authentication flow analysis, etc.

OAT-19: Account Creation

Account creation is a type of online security threat in which individuals or companies use an application's account sign-up processes to create bulk accounts for subsequent misuse. Such misuse may include content spam, spreading malware, laundering cash and goods, causing mischief, affecting brand reputation, skewing SEO, reviews, and website analytics.

Symptoms can include higher-than-average account creation rates, accounts with incomplete information relative to a typical account holder and accounts created but that are not immediately used.

Mitigation

Organizations can consider offering limited functionalities to newly created accounts for a period. Using sophisticated bot solutions with the ability to monitor and identify anomalous behavior in the account through intent analysis or progressive JavaScript challenge will be helpful in keeping the application safe from unwanted accesses.

OAT-20: Account Aggregation

Account aggregation is a process that involves collecting information from different accounts, which may include credit card accounts, bank accounts investment and other business accounts, into a single place. This aggregation application may be used by a single user to combine information from multiple applications or to combine information from various users of a single application.

Common symptoms include lack of end-user engagement, account information access behavior patterns that do not match the user profile and elevated activity peaks.

Mitigation

Every organization should identify where account aggregation would be a threat to an application and define test cases for account aggregation that confirm an application will detect and prevent users from utilizing some form of aggregation. Consider identifying and blocking IP addresses of known aggregation services.

Account aggregation is a subset of account takeover and may require specialized tools like a bot manager to differentiate between legitimate and illegitimate traffic and to block malicious programs from entering the application. Dedicated API or URL protection is also recommended, along with innovative mitigation methods such as progressively increasing JavaScript challenges to mitigate even the most sophisticated bots.

OAT-21: Denial of Inventory

Denial of inventory means depleting goods or services without completing the purchase or committing to the transaction. 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. See scalping (OAT-5). The result is direct financial loss.

Mitigation

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 intent-based behavioral analysis. Workflow and visitor journey validation are critical for mitigating threats of varying sophistication while also ensuring minimal false positives.

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.