TECHNICAL BRIEF

CHALLENGES MANAGING BOTS

SAFEGUARD AGAINST BAD BOTS, MANAGE GOOD BOTS
Bots generate a large amount of internet traffic. More than half of all bots are malevolent. Criminal bots sniff out vulnerabilities, infect and control vulnerable machines, launch denial of service attacks, steal data, commit fraud, and more. At the same time, the internet would grind to a halt without the beneficial bots that power search engines and digital assistants. Limelight WAF Advanced Bot Manager ensures maximum availability and security of web infrastructure to sustain revenue generating web traffic by eliminating malicious bot traffic while managing legitimate bot traffic.

CHALLENGE: INVASION OF THE INTERNET BOTS
Bots have officially overrun the Internet. More than half of website visits comes from automated scripts that perform repetitive tasks that would be too mundane or time-consuming for humans, according to a recent report by Statista.¹

MALICIOUS BOTS
Malicious bots do damage in many ways. The most common attacks include:

- **Reconnaissance**—Criminal bots often start with “reconnaissance missions” that look for unprotected computers to attack. Bots research targets, learning what browsers and third-party apps they use to understand the environment and its vulnerabilities.

- **Infecting and controlling vulnerable machines**—Once malicious bots find a vulnerable compute resource, they can infect that machine and report back to a Command and Control System (CnC) on the internet. The CnC system uses the victim compute resource to carry out various automated tasks. The type of compute resources that are often easy to compromise and used in botnets are home internet routers, connected cameras, and other Wi-Fi-enabled home internet devices.

- **DoS/DDoS attacks**—Bots and botnets are often used to launch network-layer denial of service (DoS) and distributed denial of service (DDoS) attacks. These attacks flood a website with requests that impact performance and can even bring the site down. In 2017, 90% of organizations acknowledged some form of activity associated with DDoS attacks, with 76% forced to contend with multiple attacks according to the Oct 2017 Neustar Cyber Security Insights Report.²

- **Layer 7 DDoS attacks**—Layer 7 DDoS attacks target the application layer. Bots send what look like actual requests from users. These attacks often go unnoticed until the site becomes overburdened and can no longer respond.

- **Spam Bot attacks**—Bots collect email addresses and hit them with tons of spam emails. Alternatively, they gather user names and passwords, employing these credentials to take over the account and use it to spread malware.

- **Injection attacks**—Injection attacks, such as Cross Site Scripting, insert malicious scripts into trusted websites which in turn deliver the scripts to the victim’s browser.

- **Stealing**—Once a bot has infected a host machine, it can steal personal and private information such as credit card numbers or bank credentials and send them back to the hacker. These attacks damage brand reputation.
• **Password guessing**—Bots can be used for brute force attacks in which they automatically attempt thousands of potential user name/password combinations until they find the right one to break into a website and wreak havoc.

• **Click fraud**—Fraudsters boost online advertising billings by automatically clicking on Internet ads, even though no human ever viewed or clicked the ads. Global advertising revenue wasted on click fraud could reach $16.4 B in 2017, according to Business Insider — more than double the $7.2 billion the Association of National Advertisers estimated was lost due to ad fraud in 2016.

• **Web Scraping**—Targeting content publishers and ecommerce sites, web scraping bots steal, exploit and sometimes republish content without authorization. For example, online retailers display prices, inventory availability, product reviews, custom photography, and product descriptions to educate customers and encourage them to purchase. Competitors might use content gleaned from web scraping to undercut prices and attract customers.

• **Cart abandonment**—Bots can run scripts that populate shopping carts and then abandon them. Genuine users will not be able to access the inventory that is held in carts by bots. This practice also skews analytics by giving internal sales teams false data that can lead them to make incorrect decisions.

**GOOD BOTS**
Although a large percentage of bots are malicious, many bots perform vital functions on the internet. This means it’s not enough to block bots, cyber security solutions must also facilitate good bots. Good bots include:

• Search engine bots that crawl websites, check links, retrieve content and update indices.

• Commercial enterprise bots that crawl websites and retrieve information.

• Feed fetcher bots that retrieve data or RSS feeds that can be displayed on websites.

• Monitoring bots that monitor various performance metrics on websites.

**FROM BOT TO WORSE**
Identifying bots is not the only challenge for website owners. For starters, web servers need protective measures that can tell a good bot from a bad bot. For example, servers might interact with a shopping bot unaware that it’s a fake meant to steal customers’ credit card numbers and other personal information. If customers find out that their financial or personal information has been compromised, an online retailer could receive a substantial blow to its brand reputation.

Worse, bots mutate constantly as cybercriminals play a game of cat and mouse with security solution vendors. As soon as a security vendor detects one type of bad bot, hackers come up with new ways around that protection. Bots have become progressively more sophisticated to circumvent detection algorithms used to uncover them.

**THE SOLUTION: THE LIMELIGHT WAF ADVANCED BOT MANAGER**
Limelight WAF Advanced Bot Manager keeps ecommerce and other sites securely up-and-running to sustain revenue generating web traffic by stopping bad bots and facilitating good bots. It also helps ensure fast customer experiences by enabling ongoing monitoring and tuning of bot management policies to protect web applications without impacting performance.

**PART OF A DEFENSE-IN-DEPTH STRATEGY**
The Limelight WAF Advanced Bot Manager is part of the Limelight Cloud Security Services architecture which delivers a defense-in-depth strategy to protect websites from cyberattacks. The comprehensive Limelight solution consists of:

• A global content delivery network (CDN) that handles large amounts of traffic with SSL and access controls including geolocation and IP white/black lists

• DDoS Attack Interceptor to easily mitigate the largest DDoS attacks.

• Web Application Firewall (WAF) with Bot Manager and API security to protect applications and web infrastructure.
COMPREHENSIVE BOT DETECTION AND MANAGEMENT CAPABILITIES
Because no one single solution can detect and intercept all malicious traffic, the Limelight Cloud Security Services offers a comprehensive suite of tools including bot detection challenges as part of Limelight’s broader defense-in-depth strategy.

BOT DETECTION
Because bots are automated scripts, many bot protection methods start by determining whether the entity requesting a connection or accessing/posting content is human.

CAPTCHA
Because it’s easy to write a script to solve simple challenges, security specialists have developed more sophisticated challenges, such as CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). A Captcha challenge presents the requestor with a picture of an object, word, number and so on, and instructs them to do something based on their understanding of the photo. For example, one popular Captcha presents 12 photos, some of which contain an object such as a car and then asks users to click on the photos containing that object. If the answer is correct, the requestor is likely to be a human.

Among Captcha’s advantages are that it is quick and easy to implement to protect sites from simple script-based Bots, such as an HTTP post flood, or bots that create random fake accounts. Most end users are also familiar with this method and how it works.

One way hackers bypass this safeguard is “Captcha as a Service” where a Captcha challenge is forwarded to a team of human responders to solve the Captcha so the malicious bot can bypass the challenge. Another downside of Captcha is that it impacts the user experience by making humans jump through hoops to use a website.

HUMAN INTERACTION CHALLENGE
To improve the user experience, developers have created the human interaction challenge, which distinguishes humans from bots by observing various behaviors indicative of human/bot traffic. The system monitors events such as where the mouse is going, where in a box the user is clicking, how much time the user spends on a site or a page, and other activities to use those observations to determine the source of the activity. For example, a bot might click on the exact same pixel in a search box each time, something humans would never do.

TECHNICAL CHALLENGES
JavaScript challenges and device fingerprinting can be used to distinguish bots from humans without demanding any action by the user or interfering with normal page operation. These solutions do not negatively impact page latency or load times.

JAVASCRIPT CHALLENGES
JavaScript is a “client-side” programming language that allows developers to convert static web pages into interactive pages. For example, you could build a JavaScript that eliminates the need for visitors to fill out an entire form and submit it before being informed they made a typo; JavaScript can validate each field as it is entered. Standard web browsers are able to read, interpret, and execute JavaScript scripts. Bots, however, typically do not run JavaScript. The JavaScript challenge therefore tests to see if JavaScript will run on the browser; if it doesn’t, the browser fails the challenge.

DEVICE FINGERPRINTING
Device fingerprinting observes the device a website request comes from. Few legitimate machines share all the same characteristics, such as browser and version, OS and version, and other software in use. The device fingerprinting challenge observes 50+ characteristics of the device and generates a unique hash to identify that machine.

Most bots mimic a browser (and all its attributes) and use the same script on hundreds or thousands of machines. If 100, 500, or more users attempt to access a site using the same hash, it’s likely that they are all being controlled by a command and control server somewhere else. Device fingerprinting makes it easy to identify large numbers of machines being used to run the same script.
BEST PRACTICES BOT MANAGEMENT
Having a variety of bot detection mechanisms that include human interaction challenges (CAPTCHA, behavioral usage patterns) as well as machine-based challenges (JavaScript, device fingerprinting, traffic shaping) is the optimal way to separate good bots from bad bots.

DEFENSIVE CAPABILITIES
TRAFFIC SHAPING
If a site becomes overwhelmed with rapid-fire requests, legitimate traffic will be unable to get through. Traffic shaping (also known as IP Rate limiting) observes the rate at which requests are coming through and limits which requests for connection are fulfilled to reserve enough bandwidth for legitimate traffic. IP rate limiting can be used to prevent DoS attacks or spam email attacks.

WHITE LISTING
White listing allows you to specify known good bots that will be allowed through the WAF without challenges. White listed bots can access the site as quickly and as often as they want.

BOT MANAGER IMPLEMENTATION
In addition to managing bot traffic, the Limelight WAF Advanced Bot Manager offers capabilities that make the solution simple to implement, deploy and administer. Hosted in the cloud, this flexible solution eliminates the need for IT organizations to install and manage hardware and software. Capabilities that enable ongoing monitoring and tuning of bot management policies ensure you always have the optimal security profile to protect your web applications without impacting performance. A real-time dashboard, reporting, analytics and alerts notify your security personnel of any bot attacks so they can quickly remediate the situation.

BENEFITS
Limelight WAF Advanced Bot Manager helps you:

• Protect brand reputation—Security breaches have a lasting impact on brand reputation, with more than 40% of consumers saying they will no longer make online transactions with a web site that has been previously breached. Protect your brand reputation by strengthening web application security by identifying and eliminating bad bots and protecting customer data from intrusion.

• Keep customers coming back for more—Consumers have higher engagement with web sites that offer faster performance. Improve user experience by blocking resource-draining bots and providing the fastest online experiences.

• Defend against emerging security threats—Ongoing monitoring and tuning of bot management policies ensures an optimal security profile to protect web applications against new and emerging threats.

PROTECT YOUR WEBSITE FROM MALICIOUS BOTS
Learn more about how Limelight WAF Advanced Bot Manager can keep your sites secure, available, and open for business by blocking malicious bots while facilitating good bots. Contact us at: +1 602 850 5000, Option 1. Or info@llnw.com.
ABOUT THE ORCHESTRATE PLATFORM

The Limelight Orchestrate Platform is built upon a global, private backbone network with the speed, capacity, and availability to deliver the experiences today’s audiences demand. This industry-leading Platform includes integrated content delivery, web acceleration, origin storage, video management, cloud security, and support services. The unique combination of global private infrastructure, advanced software, and expert services surpasses other CDNs, to enable today’s and tomorrow’s workflows and put audience experience first.

ABOUT LIMELIGHT NETWORKS

Limelight Networks (NASDAQ: LLNW), a global leader in digital content delivery, empowers customers to better engage online audiences by enabling them to securely manage and globally deliver digital content, on virtually any device. For more information visit our website at https://www.limelight.com.

1 https://www.statista.com/statistics/670782/bot-traffic-share/

