

ULTIMATE GUIDE TO

BOT MANAGEMENT



TABLE OF CONTENTS

CHAPTER	TOPIC AND KEY QUESTIONS ADDRESSED	
PREFACE		03
1.0	OVERVIEW	04
	Bot Basics	
	Good Bots: Beneficial to Online Businesses	
	Bad Bots: Up to No Good	
	HTTP vs. IoT Botnet: What's the Difference?	
	Business Impacts of Bad Bots: How Bots Impact Various Industries and Business Functions	
	Industry-Specific Impacts	
	Some of the Most Well-Known "Celebrity" Bot Attacks	
2.0	FOUR GENERATIONS OF BOTS	10
	First Generation: A Closer Look	
	Second Generation: A Closer Look	
	Third Generation: A Closer Look	
	Fourth Generation: A Closer Look	
3.0	TECHNICAL OVERVIEW: BOT TYPES BY CHANNEL	18
	APIs	
	APIs Under Siege	
	Mobile Apps	
	Websites	
4.0	DETECTION & MITIGATION TECHNIQUES	22
	Detection	
	Mitigation	
	A Healthy Bot Management Strategy	
	Deployment Options	
5.0	ADDITIONAL CONSIDERATIONS	26
	WAF or Bot Management?	
6.0	BUYERS CHECKLIST	28
	Key Considerations When Evaluating Bot Management Solutions	
CLOSING		30
APPENDIX		31
	OWASP Top 21 Automated Threats	
	How to Evaluate Bot Management Solutions	
	The Top Free and Paid Web Scraping Tools and Services	
	The 50 Most Common Web Scraping Tools	
	Contact Us	
	For More Information	

PREFACE

BOTS TOUCH VIRTUALLY EVERY PART OF OUR DIGITAL LIVES — AND NOW ACCOUNT FOR OVER HALF OF ALL WEB TRAFFIC.¹

Some help populate our news feeds, tell the weather, provide stock quotes and control search rankings. We use bots to book travel, access online customer support, even to turn our lights on and off and unlock our doors.

But other bots are designed for more mischievous purposes — including account takeover, content scraping, payment fraud and denial-of-service (DoS) attacks. These bots account for as much as 26% of total internet traffic, and their attacks are often carried out by competitors looking to undermine your competitive advantage, steal your information or increase your online marketing costs.² These “bad bots” represent one of the fastest-growing and gravest threats to websites, mobile applications and application programming interfaces (APIs).

This e-book provides an overview of evolving bot threats, outlines options for detection and mitigation and offers a concise buyers guide to help evaluate potential bot management solutions.

¹Application Security in a Digitally Connected World, Nov. 2017, Radware
²Application Security in a Digitally Connected World, Nov. 2017, Radware

Overview

BOT BASICS

BOTS ARE AUTOMATED PROGRAMS CREATED TO PERFORM REPETITIVE TASKS. WITH THE COMPUTING POWER AVAILABLE TO THEM, PROGRAMMERS CAN CREATE BOTS TO EXECUTE TASKS AT VERY HIGH SPEEDS — SO HIGH, IN FACT, IT'S UNTHINKABLE FOR A HUMAN TO KEEP PACE WHEN DOING THE SAME TASKS.

Although bots have been in use for about five decades, modern bots are a complicated bunch. Some are immensely helpful; others are harmful by design.

GOOD BOTS: BENEFICIAL TO ONLINE BUSINESSES

Good bots are legitimate bots whose actions are beneficial. These bots crawl a website to support search engine optimization (SEO), aggregation and market intelligence/analytics.

Here are some general categories of good bots and the functions they perform:

Monitoring bots (example: Pingdom) monitor websites' uptime and system health — periodically checking and reporting on page load times and downtime duration, among other metrics.

Backlink checker bots (example: UASlinkChecker) confirm the inbound URLs that a website is getting, so marketers and SEO specialists can understand trends and optimize pages accordingly.

Social network bots (example: Facebook bot) are run by social networking websites that give visibility to your website and drive engagement on their platforms.

Partner bots (example: PayPal IPN) enable important functionality on websites that are transactional in nature.

Aggregator/Feedfetcher bots (example: WikioFeedBot) collate information from websites and keep users or subscribers updated on news, events or blog posts.

Search engine crawler bots (also known as spiders) crawl and index webpages, making them available on search engines, such as Google and Bing. You can control their crawl rates, as well as specify rules in the robots.txt. Search crawlers will then follow your rules when indexing your webpages. Search engine crawler bots are essential to indexing your webpage so that it becomes visible to everyone using the internet. Without them, most online businesses would struggle to establish their brand value and attract new customers.

Many of these good bots are highly beneficial – if not critical – to your business. They play important roles in establishing and maintaining your online presence and enabling a favorable customer experience. While you may decide to selectively stop one or more of them, blocking them could reduce the visibility your website gets on search engines and other social platforms.

BAD BOTS: UP TO NO GOOD

Bad bots are automated programs that don't play by the rules. Mostly unregulated, they have a definite "malicious" pattern. For example, imagine thousands of page visits originating from a single IP address within a very short period of time. That activity stresses web servers, chokes available bandwidth and directly impacts genuine users trying to access a product or service on a website. And that's just one example of how bad bots can wreak havoc on a website and business.

Here are some general categories of bad bots and the havoc they can wreak on business:



SCRAPER BOTS

Scraper bots can be sent by third-party scrapers or competitors to steal information from your website – even content unique to your business. That might include product reviews, breaking news, dynamic pricing information of products listed, a product catalog or even user-generated content on community forums. By scraping your content and then publishing it elsewhere, bots can affect your website's search engine rankings. There have been instances of stolen content outranking the original on Google search pages. This theft directly impacts the bottom line of companies that have invested budget and resources to create original content.



SPAM BOTS

Spam bots primarily target community portals, blog comment sections and lead collection forms. They arrive in the middle of user conversations and insert unwanted ads, links and banners. These insertions frustrate genuine users who are participating in forums and commenting on blog posts. What's more, spam bots insert links that may be malicious – for example, directing users to phishing sites that may persuade them to divulge sensitive information, such as bank account numbers and passcodes.



SCALPER BOTS

Scalper bots target ticketing websites and make bulk purchases. The modus operandi is to buy hundreds of tickets as soon as the bookings open and then sell them to reseller websites at many times the original ticket price. They emulate humanlike behavior to remain undetected by conventional or in-house bot detection methodologies.



HTTP VS. IOT BOTNET: WHAT'S THE DIFFERENCE?

Depending on a person's background, bots and botnets have different meanings. For some, the word "botnet" conjures up a picture of a distributed denial-of-service (DDoS) attack involving vast numbers of internet of things (IoT) devices. While DDoS can be a widespread attack originating from botnets, botnets are known to carry various payloads and are used in various types of attacks.

Of the known botnets, some are used to mine cryptocurrency on infected devices. Others use infected devices as anonymizing proxies to conceal attacks or illegal activity. Still others use infected devices as mail relays for massive spam campaigns. The threat emerging from botnets is only limited by the creativity of their creators.

In this guide, we discuss bots and botnets and how they are used to perform attacks against online services or to deliver a legitimate service to an online service. It is important to emphasize that legitimate bots provide advantages or services and are considered "good bots." "Bad bots," on the other hand, perform attacks against websites and APIs. Both types of bots leverage the same HTTP protocols, meaning that the tactics and methods to provide a righteous service can be identical to those used for malicious intent.

Attacks from bad bots are as diverse as they are frequent. They include clicker bots that perform ad fraud, spam bots that illegally post advertisements, web scrapers, and bots that try to exhaust an e-commerce site's inventory. These are the kinds of bad bots that affect many online commercial and noncommercial services.

In the remainder of this document, we generally refer to bots and specifically indicate HTTP bots as devices or programs that primarily use the HTTP protocols for malicious or legitimate behavior against an online website or API.

BUSINESS IMPACTS OF BAD BOTS: HOW BOTS IMPACT VARIOUS INDUSTRIES AND BUSINESS FUNCTIONS

Any company with an e-commerce presence must prepare to detect and mitigate bad bots seeking to execute any or all of these attacks:

Account Takeover

Scammers use bots to make fraudulent purchases using stolen user credentials. Hackers target user accounts to harvest personal information and purchase history. They can also make unauthorized transfers of virtual currencies — from reward points and wallet money to gift cards and air miles.

Carding

Scammers use bots to test thousands of stolen credit card numbers against a merchant's payment processes. Since owners of stolen cards can claim a refund for the fraudulent transaction, carding attacks lead to chargebacks, penalties and poor merchant history. Frequent carding activities and too many chargebacks can eventually result in a merchant being prevented from accepting credit cards.



SCANNING..

Scraping of Pricing, Content and Inventory Information

Competitors scrape prices and product listings to attract your customers. Such aggressive tactics sabotage a retailer's revenue stream. Scraping of unique and proprietary content is another common problem for online businesses. Duplication of exclusive content can negatively impact SEO efforts as well.

Cart Abandonment and Inventory Exhaustion

Competitors' bots add hundreds of items to carts and abandon them later to prevent real consumers from buying products. These automated attacks create artificial inventory exhaustion, reduce sales, skew conversion rates and hurt brand reputation.

Application DDoS

Application DDoS attacks affect the availability of websites. The surge in nonhuman traffic on checkout pages can increase the load on inventory databases and payment processing resources. Botnets perform large-scale Layer 7 DDoS attacks that are often "low and slow" (that is, making just one or two hits per IP address used) to go undetected by conventional security measures. DDoS attacks also create a poor buying experience for customers.

Scalping Products and Tickets

Malicious bots are active during sales and buy valuable goods, such as consumer electronics, to resell later at a much higher price. Bots are deployed to scoop up tickets for popular events as soon as they go on sale.

Fake Account Creation

Criminals employ bots to create fake accounts to commit various forms of cybercrime, such as content spam, laundering virtual cash, spreading malware and skewing surveys and SEO.

INDUSTRY-SPECIFIC IMPACTS

Bots fuel distinctive sets of challenges for these types of organizations:

Advertising Networks and Digital Publishers

Scammers use botnets to generate false clicks and to support fraudulent displays of digital ads. Fake traffic artificially inflates advertising costs. Bots also perform retargeting fraud to illegally monetize the invalid traffic on publishing sites. Such attacks sabotage ad networks' efforts to connect advertisers with quality inventory, help marketers reach a wider audience and offer customers more value from campaigns. Ultimately, bad bots generate invalid traffic that adversely affects an ad network's brand reputation and undermines its claim of providing a trustworthy media buying environment.

Financial Services

Banking, financial services and insurance organizations represent high-value targets for scammers. The use of botnets to commit fraud has ramped up the speed of attacks in recent years. Hackers deploy botnets on financial institutions to take over accounts, execute DDoS attacks or scrape content. Again, large-scale sophisticated bots are often low and slow to bypass conventional security measures.



Marketplace and Classifieds

The essential asset for any classified site is fresh content and unique listings. Malicious bots sent by competitors and third-party scrapers crawl information from these websites to publish it elsewhere or even sell it. In addition to stealing new listings, malicious bots fill web forms with fake details, ending up as dead leads that don't convert. Sales teams may waste a significant amount of time and effort chasing them. Eventually, these bad bots also skew analytics — and drive down server performance.

Travel

Scraper bots are the most obvious threat for online travel websites. Scraper bots can be deployed by competitors and scammers to scrape dynamic pricing of airline tickets. Scraping pricing information can give competitors an unfair advantage and prove to be a long-term business loss. Keeping pricing safe from competitors is critical to retaining customers, partners and brand competitiveness. Another threat: fake queries for flight tickets. Costs levied by the airline global distribution system (GDS) will increase significantly because of fake GDS queries made by bots. Competitors can use these fake queries to scrape ticket prices. These fake queries cost a travel company money — and none of these queries will ever generate a legitimate booking.



SCANNING..

SOME OF THE MOST WELL-KNOWN “CELEBRITY” BOT ATTACKS

Many bots never gain acclaim for their mischief. These, however, made headlines:



2019

APR

Scalpers were selling tickets for the hotly anticipated movie **Avengers: Endgame**³ the same day tickets went on sale, at highly inflated prices. Earlier in 2019, other victims of scalping campaigns included famous artists such as the **Korean boy band BTS**⁴ and **British singer Ed Sheeran**⁵. Back in 2015, **Coldplay**⁶ fans found their favorite band's tickets resold at a 3,000% premium.

FEB

Ryanair, a low-cost carrier based in Ireland, filed a U.S. lawsuit against **Expedia** over screen scraping. The suit argues that Expedia's unauthorized web scraping of the airline's site violates the U.S. Computer Fraud and Abuse Act (CFAA). Ryanair further asserts that Expedia caused reputational damage to the airline by levying opaque fees on consumers and that Expedia's unauthorized activities tax Ryanair's website, causing poor response times and other errors.⁷

2018

NOV

The FBI, the Department of Homeland Security, Google and other private security companies disrupted a major ad-fraud network. **3ve** involved 1.7 million IP addresses and caused tens of millions of dollars in losses. At its peak, the 3ve botnet consisted of more than 700,000 compromised machines and more than 60,000 accounts selling garbage ad inventory.⁸

SEP

British Airways⁹ (BA) was the victim of a data breach potentially affecting 380,000 customers. Just five lines of JavaScript code were added by the attackers to existing JavaScript libraries hosted on the web server. The five-line bot executed in the context of the client browser and hooked into the payment form submission event, giving the bot access to submitted credit card information, including the card's verification code, before it was sent to BA's payment processing service. The information was scraped and stored on a server created and hosted by the attackers. The attack was linked to Magecart, which previously affected a breadth of providers including **AdMaxim, CloudCMS and Picreel**¹⁰ through a large-scale, automated, web-based supply chain attack. In July 2019, a Magecart group was injecting skimmer code in JavaScript libraries from third-party web suppliers that were storing their scripts in world-writable Amazon Simple Storage Service (S3) buckets, potentially affecting several thousands of websites using the services of these providers.¹¹

APR

For about eight months, **Panerabread.com** was leaking customer records in plain text, affecting as many as 7 million people who had signed up to order food through the fast-casual chain's website. A security vulnerability in one of the APIs that the company uses across its digital platforms made it potentially simple for anyone to scrape all available customer records using a basic script.¹²

2017

JUN

A police raid in Thailand provided a glimpse of the underbelly of the internet: primitive metal shelving holding 500 smartphones, each wired to a computer monitor for the purposes of click fraud. This and other **click fraud farms** profit by generating fake traffic that makes websites, social media posts and advertisements appear to be more popular than they actually are.¹³

MAR

A **McDonald's** India app, McDelivery, was leaking the personal data of more than 2.2 million users. An unprotected and publicly accessible API made it possible to get user details. That, along with serially enumerable integers as customer IDs, makes it far too easy for anyone to scrape the personal data off all the site's registered users.¹⁴

2016

MAY

Cambridge Analytica scraped the personal information of 87 million U.S. residents from Facebook and leveraged data science on the scraped information to target residents with custom Facebook ad campaigns in an attempt to influence their voting behavior.¹⁵

³<https://www.asiaone.com/singapore/scalpers-selling-tickets-avengers-endgame-888-carouseil>

⁴<https://mustsharenews.com/bts-ticket-scalpers/>

⁵<https://theindustryobserver.thebrag.com/ed-sheeran-cancels-tickets-fight-scalpers/>

⁶<https://www.cnbc.com/2016/11/23/sold-out-coldplay-concert-tickets-in-singapore-being-resold-at-3000-premium-by-scalpers.html>

⁷<https://skift.com/2018/02/25/ryanair-files-u-s-lawsuit-against-expedia-over-screen-scraping/>

⁸<https://digitalguardian.com/blog/all-about-3ve>

⁹<https://www.riskiq.com/blog/labs/magecart-british-airways-breach/>

¹⁰<https://www.riskiq.com/blog/labs/cloudcms-picreel-magecart/>

¹¹<https://www.riskiq.com/blog/labs/magecart-amazon-s3-buckets/>

¹²<https://www.csoonline.com/article/3268025/panera-bread-blew-off-breach-report-for-8-months-leaked-millions-of-customer-records.html>

¹³https://www.vice.com/en_us/article/43yqdd/look-at-this-massive-click-fraud-farm-that-was-just-busted-in-thailand

¹⁴<https://www.securityweek.com/mcdonalds-app-leaks-details-22-million-customers>

¹⁵<https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>



2.0

Four Generations of Bots

WITH THE ESCALATING RACE BETWEEN BOT DEVELOPERS AND SECURITY EXPERTS — ALONG WITH THE INCREASING USE OF JAVASCRIPT AND HTML5 WEB TECHNOLOGIES — BOTS HAVE EVOLVED SIGNIFICANTLY FROM THEIR ORIGINS AS SIMPLE SCRIPTING TOOLS THAT USED COMMAND LINE INTERFACES.

Bots now leverage full-fledged browsers and are programmed to mimic human behavior in the way they traverse a website or application, move the mouse, tap and swipe on mobile devices and generally try to simulate real visitors to evade security systems.

This chapter looks back at the first three generations of HTTP bots and provides an overview of current fourth-generation bots.



SCANNING...

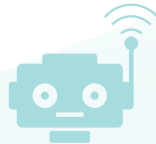
FIGURE 1. EVOLUTION OF BOTS

FIRST GENERATION



- Typically use just one or two IP addresses to execute thousands of webpage visits to scrape content or spam forms
- Easy to detect and blacklist thanks to repetitive attack patterns and the small number of originating IP addresses

SECOND GENERATION



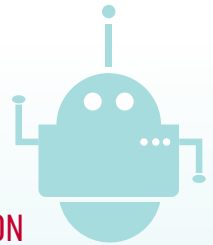
- Leverage “headless browsers” — which are essentially website development and testing tools — to tap into their ability to run JavaScript and maintain cookies

THIRD GENERATION

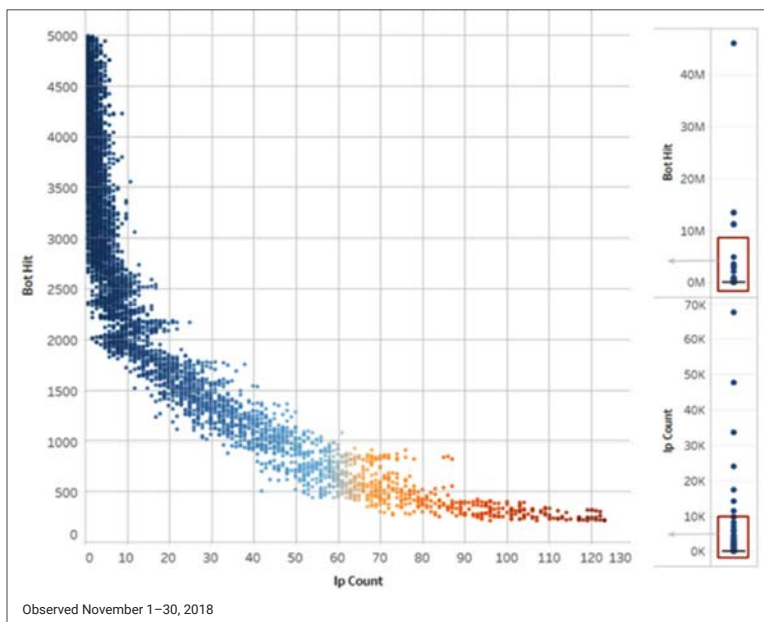


- Perform simple actions, such as moving the mouse, scrolling and clicking links to traverse a website
- Exhibit sophisticated behaviors that may overcome certain challenges but still cannot overcome interaction-based detection (examples: CAPTCHA or invisible challenges)

FOURTH GENERATION



- Rotate through large numbers of user agents (UAs) and device IDs — making just a few hits from each to avoid detection
- Make random mouse movements (not just in a straight line like third-generation bots) and other humanlike browsing characteristics
- Record real user interactions, such as taps and swipes, on hijacked or malware-laden mobile apps, so they can be replicated, “blend in” with human traffic and circumvent security measures

FIGURE 2. BASIC VS. SOPHISTICATED BOTS: HITS PER IP ADDRESS¹⁶

First- and second-generation bots typically use very few IP addresses and make thousands of hits from each one. On the other hand, third- and fourth-generation bots can rotate through thousands of IP addresses. As a result, they make only one or two hits from each address. This evasion technique, known as “low and slow,” enables them to slip past basic security systems.

¹⁶Data from analysis of website traffic of an American e-commerce company

**FIRST GENERATION:
A CLOSER LOOK**

Definition: First-generation bots were built with basic scripting tools and make cURL-like requests to websites using a small number of IP addresses (often just one or two). They do not have the ability to store cookies or execute JavaScript, so they do not possess the capabilities of a real web browser.

Impact: These bots are generally used to carry out scraping, carding and form spam.

Mitigation: These simple bots generally originate from data centers and use proxy IP addresses and inconsistent UAs. They often make thousands of hits from just one or two IP addresses. They also operate through scraping tools, such as ScreamingFrog and DeepCrawl. They are the easiest to detect since they cannot maintain cookies, which most websites use. In addition, they fail JavaScript challenges because they cannot execute them. First-generation bots can be blocked by blacklisting their IP addresses and UAs, as well as combinations of IPs and UAs.

FIGURE 3. DISPARITY OF NUMBER OF IPs USED BY SOPHISTICATED BOTS (GENERATION 3 AND 4) VERSUS BASIC BOTS (GENERATION 1 AND 2)¹⁷

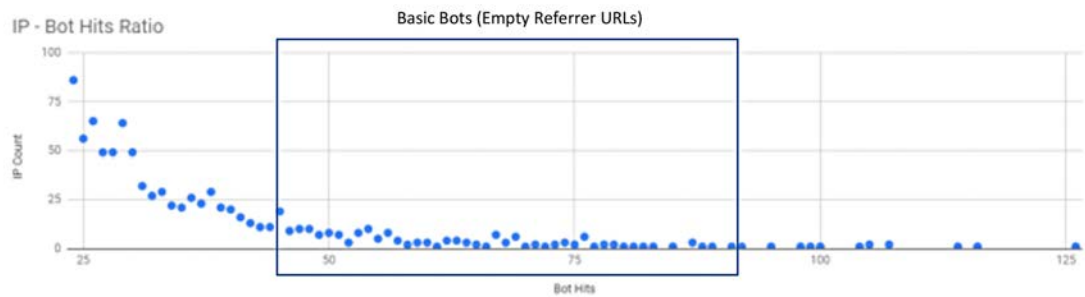


FIGURE 4. THE MAJORITY OF BAD BOT TRAFFIC TO THESE WEBSITES WERE FIRST-GENERATION BOTS¹⁸

DOMAIN	BOT %
dtlbs.ru	97.50%
alibaba.com	93.94%
ovh.com	90.18%

These stats are from across our client base, January–December 2018.

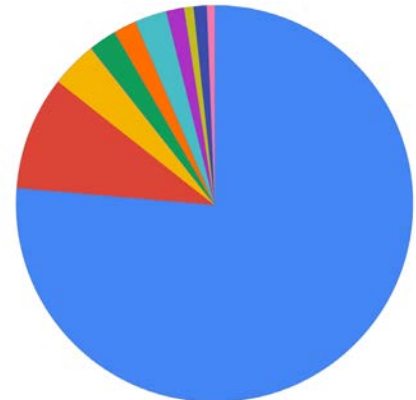


¹⁷Data from analysis of website traffic of an international publishing company
¹⁸Data from analysis of website traffic from Radware clients

FIGURE 5. OVERVIEW OF OUTDATED WEB BROWSERS USED BY FIRST-GENERATION BOTS

First-generation bots usually have UAs from outdated versions of popular browsers such as Google Chrome, Firefox and Internet Explorer. They cannot run JavaScript or store cookies.

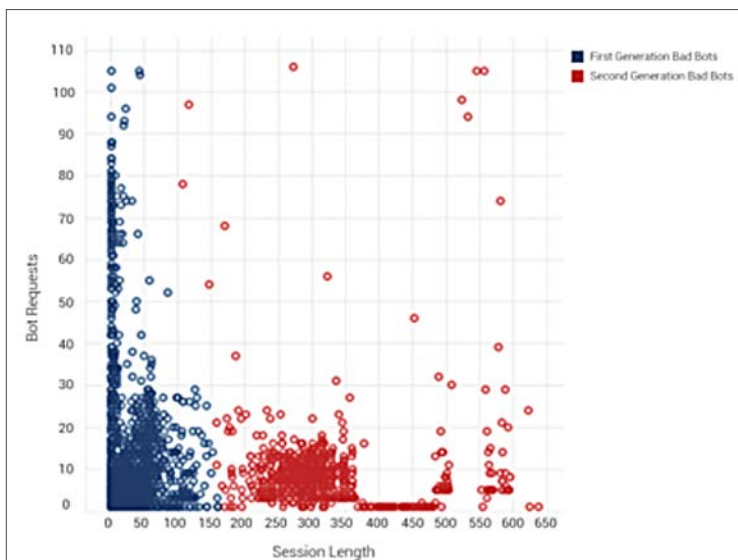
- Chrome 41.0.2228.0
- Chrome 59.0.3053.3
- Chrome 50.0.2661.102
- Chrome 43.0.2357.81
- Chrome 63.0.3239.84
- Firefox 29.0
- IE 11.0
- Safari Mobile 11.0
- Chrome 66.0.3359.181
- Firefox 55.0



Source data is from Radware Bot Manager subscriber IDs.

FIGURE 6. CONTRAST BETWEEN FIRST- AND SECOND-GENERATION BOTS

Second-generation bots (plotted in red) can load cookies and JavaScript. Compared to first-generation bots (plotted in blue), generally their visits have a longer session length, although they make fewer hits per session.



SECOND GENERATION: A CLOSER LOOK

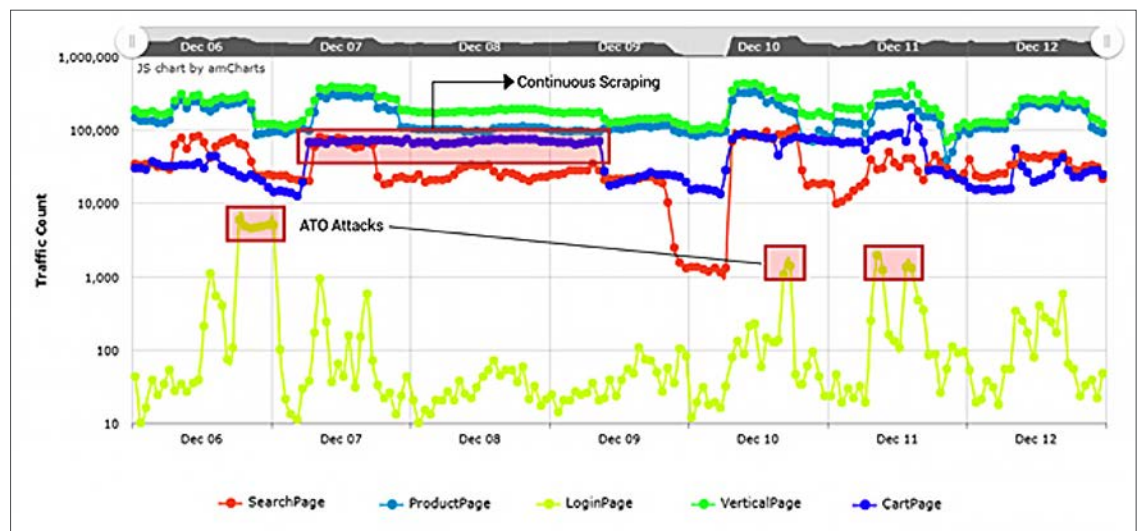
Definition: These bots operate through website development and testing tools known as “headless” browsers (examples: PhantomJS and Simple-Browser), as well as later versions of Chrome and Firefox, which allow for operation in headless mode. Unlike first-generation bots, they can maintain cookies and execute JavaScript. Botmasters began using headless browsers in response to the growing use of JavaScript challenges in websites and applications.

Impact: These bots are used for application DDoS attacks, scraping, form spam, skewed analytics and ad fraud.

Mitigation: These bots can be identified through their browser and device characteristics, including the presence of specific JavaScript variables, iframe tampering, sessions and cookies. Once the bot is identified, it can be blocked based on its fingerprints. Another method of detecting these bots is to analyze metrics and typical user journeys and then look for large discrepancies in the traffic across different sections of a website. Those discrepancies can provide telltale signs of bots intending to carry out different types of attacks, such as account takeover and scraping (see Figure 7).

FIGURE 7. TRAFFIC VARIATIONS ACROSS SECTIONS OF A WEBSITE CAN REVEAL TELLTALE SIGNS OF AN ATTACK¹⁹

Most real website and app users exhibit consistent patterns. They generally start at the login page and then move on to search pages or product pages. They typically conclude by adding products to the shopping cart and paying for their purchase — or exiting the website without buying. Bots programmed to carry out account takeover and scraping attacks have page traversal patterns noticeably different from those of genuine visitors.



¹⁹Data from analysis of website traffic of an American e-commerce company

THIRD GENERATION: A CLOSER LOOK

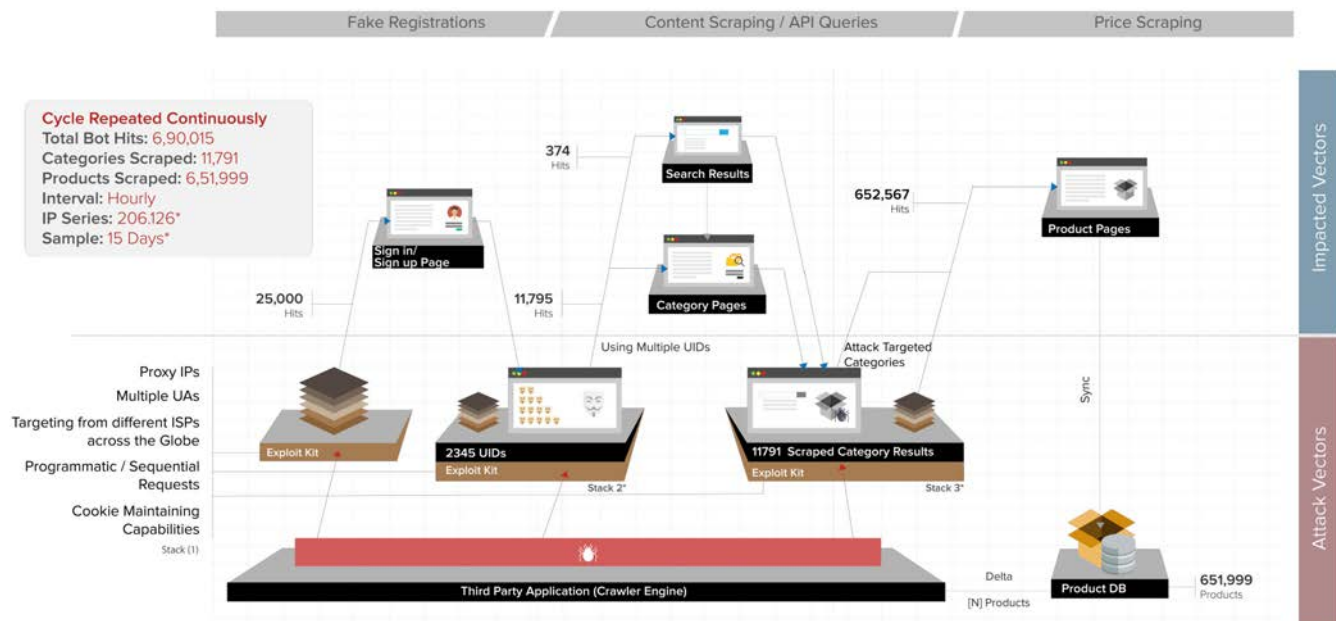
Definition: These bots use full-fledged browsers – dedicated or hijacked by malware – for their operation. They can simulate basic humanlike interactions, such as simple mouse movements and keystrokes. However, they may fail to demonstrate humanlike randomness in their behavior.

Impact: Third-generation bots are used for account takeover, application DDoS, API abuse, carding and ad fraud, among other purposes.

Mitigation: Third-generation bots are difficult to detect based on device and browser characteristics. Interaction-based user behavioral analysis is required to detect such bots, which generally follow a programmatic sequence of URL traversals. Figure 8 outlines the attack strategy that third-generation bots use to carry out scraping attacks.

FIGURE 8. EXAMPLE OF A THIRD-GENERATION BOT SCRAPING ATTACK²⁰

In this representation of a large attempted scraping attack on a retailer, third-generation bots leveraged multiple IP addresses and user agents and originated from several ISPs across the globe in a coordinated manner.



²⁰Data from analysis of website traffic of an American e-commerce company

FOURTH GENERATION: A CLOSER LOOK

Definition: The latest generation of bots have advanced humanlike interaction characteristics — including moving the mouse pointer in a random, humanlike pattern instead of in straight lines. These bots also can change their UAs while rotating through thousands of IP addresses. There is growing evidence that points to bot developers carrying out “behavior hijacking” — recording the way in which real users touch and swipe on hijacked mobile apps to more closely mimic human behavior on a website or app. Behavior hijacking makes them much harder to detect, as their activities cannot easily be differentiated from those of real users. What’s more, their wide distribution is attributable to the large number of users whose browsers and devices have been hijacked.

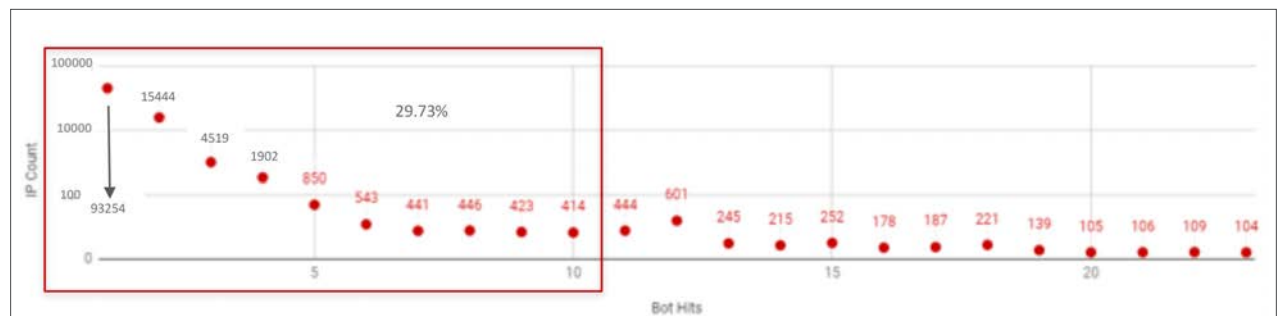
Impact: Fourth-generation bots are used for account takeover, application DDoS, API abuse, carding and ad fraud.

Mitigation: These bots are massively distributed across tens of thousands of IP addresses, often carrying out “low and slow” attacks to slip past security measures. Detecting these bots based on shallow interaction characteristics, such as mouse movement patterns, will result in a high number of false positives. Prevailing techniques are therefore inadequate for mitigating such bots. Machine learning-based technologies, such as intent-based deep behavioral analysis (IDBA) — which are semi-supervised machine learning models to identify the intent of bots with the highest precision — are required to accurately detect fourth-generation bots with zero false positives.

Such analysis spans the visitor’s journey through the entire web property — with a focus on interaction patterns, such as mouse movements, scrolling and taps, along with the sequence of URLs traversed, the referrers used and the time spent at each page. This analysis should also capture additional parameters related to the browser stack, IP reputation, fingerprints and other characteristics.

FIGURE 9. OVERVIEW OF IP ADDRESSES USED BY FOURTH-GENERATION BOTS, WHICH USE MANY IPs BUT ONLY MAKE A FEW HITS FROM EACH ONE²¹

Operating through a large and globally distributed number of IP addresses and often hijacked browsers, fourth-generation bots can sneak past basic security systems by making very few hits per IP address used. This approach allows their traffic to blend in with that of real users.



²¹Data from analysis of website traffic of an international publishing company

FIGURE 10. OVERVIEW OF HOW FOURTH-GENERATION BOTS ROTATE THROUGH THOUSANDS OF IP ADDRESSES AND DEVICE IDs TO EVADE DETECTION²²

To be camouflaged among genuine visitors, fourth-generation bots present themselves with a multitude of IP addresses and device IDs. This example of an actual attempted bot attack reveals how they leverage multiple IP addresses while using one device ID, as well as employing thousands of device IDs while using just one IP address.

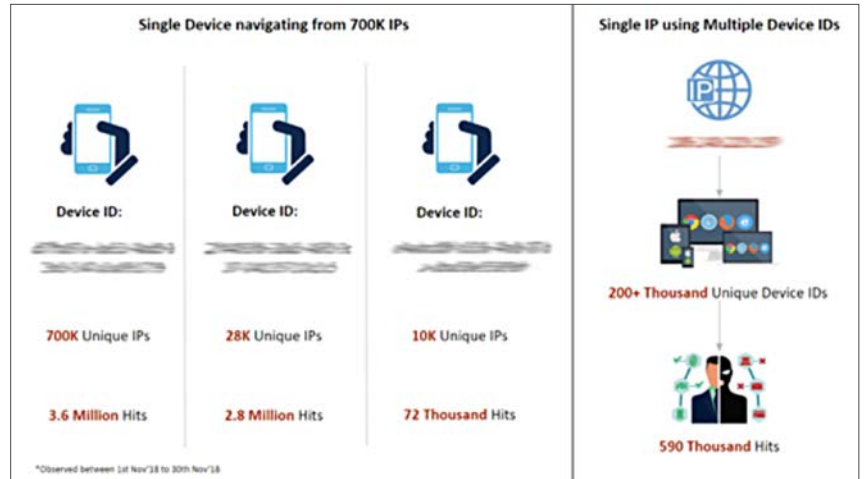
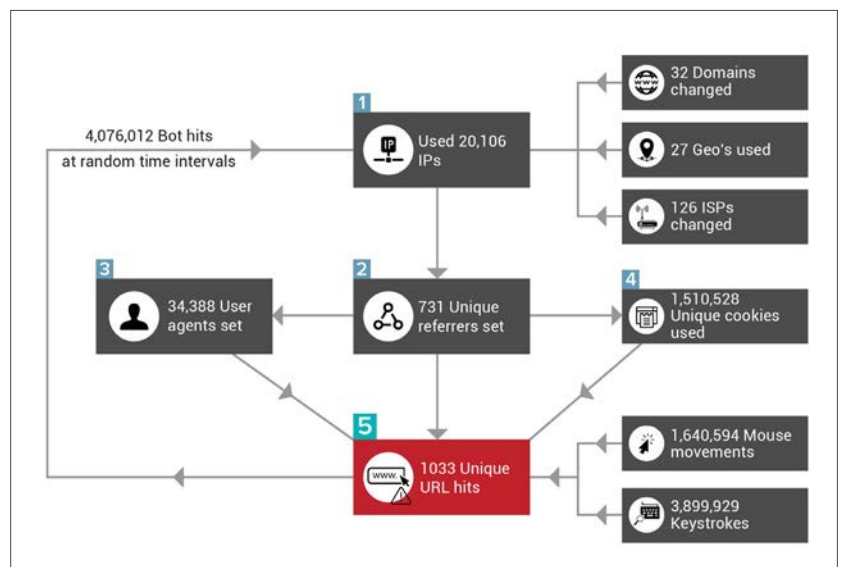


FIGURE 11. EXAMPLE OF AN ATTACK BY A FOURTH-GENERATION BOT FOR ACCOUNT TAKEOVER²³

An actual account takeover attempt on a client's website reveals the multitude of ISPs, geographical origins, domains, user agents and cookies that were leveraged along with millions of keystrokes and mouse movements (obtained through behavior hijacking) to make more than 4 million hits.



²²Data from analysis of website traffic of a social media company

²³Data from analysis of website traffic of an American e-commerce company

3.0

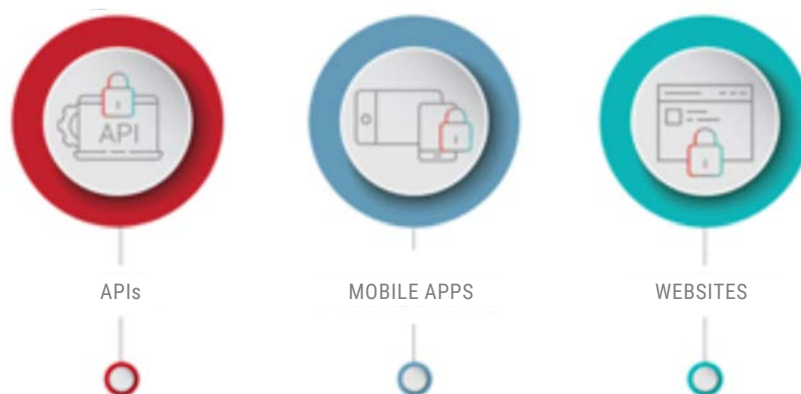
Technical Overview: Bot Types by Channel

WAYS IN WHICH BOTS CAN INFILTRATE THE THREE MAIN CHANNELS OF THE ONLINE WORLD:

- **APIs**, which provide access to machine-to-machine communications and frequently involve high volumes of calls, making them easier targets for bot attacks
- **Mobile apps**, which can be exploited by bots to wage attacks on online services that the apps interact with to provide content to users
- **Websites**, which present content in human-readable formats, which must be scraped and translated into machine-readable formats for use by bots

These channels are highly interconnected – with APIs playing a major role and fueling major risks when it comes to bot management.

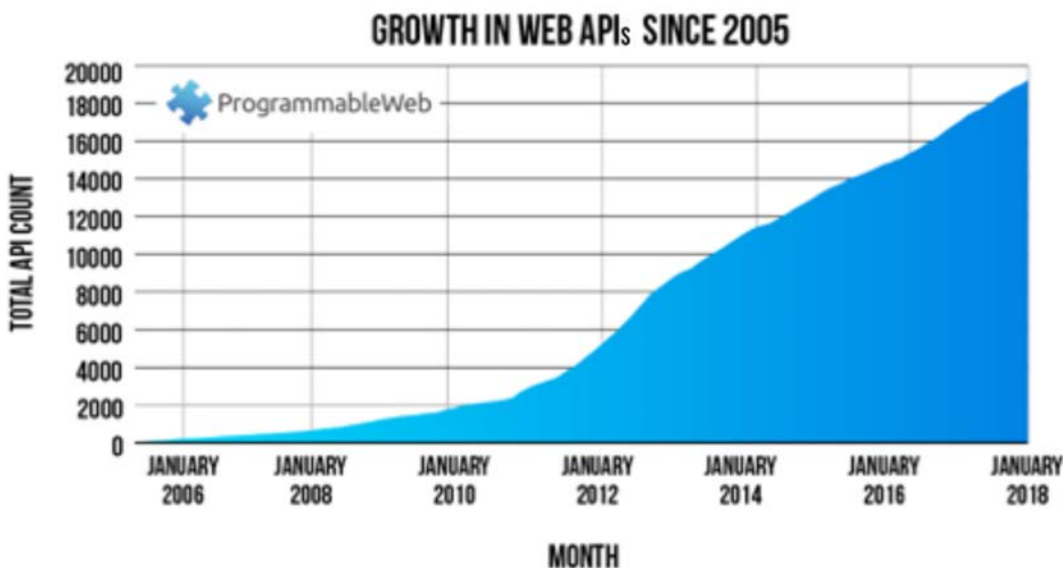
BOTS TARGET ALL CHANNELS



APIs

APIs are software intermediaries that make it possible for systems to communicate with each other. Use of web APIs has grown exponentially since 2005 (see Figure 12). In fact, it's safe to say that APIs are — and will continue to be — everywhere. They are critical enablers of countless systems and services. APIs power organizations' back-end systems, mobile apps and increasingly even websites — and will become even more critical as the IoT continues to connect everything from toasters to cars.

FIGURE 12. GROWTH IN WEB APIs SINCE 2005²⁴



API growth has been significant to date, and several industry trends will further fuel use of APIs:

- **IoT:** The industry is poised for an IoT explosion through 5G. IoT and industrial IoT solutions will connect to clouds directly. Cloud APIs supporting telemetry registration (sensors) and rich functionality (example: If This Then That (IFTTT), Alexa and Google Assistant) will be exposed directly.
- **Mobile apps:** IoT and 5G networking will also fuel the growth in mobile applications and their reliance on APIs.
- **Cloud migrations:** As these migrations continue accelerating, multicloud environments are a fact of life. Applications can mix and match best-in-class services from Amazon Web Services (AWS), Azure and Google Cloud. All these interconnecting cloud applications require APIs.

As organizations create APIs to power their businesses, they sometimes decide to make the API available for sale and use by other enterprises. This practice is fueling a fast-growing “API economy” alongside the trends in IoT, 5G and the cloud.

²⁴<https://www.programmableweb.com/news/apis-show-faster-growth-rate-2019-previous-years/research/2019/07/17>

The trouble is, APIs can be highly vulnerable, making them frequent attack targets. And because APIs are powered by machine-to-machine communication, it can be far more difficult to determine if an API call is originating from a good source for a helpful purpose — or from a bad actor with ill intentions for your business and your customers. That’s because APIs are *built* for machines to talk to, making the threshold for bots interacting easier with an API than with a website. Bots don’t have to mimic users or scrape and decode PDFs or HTML tables; they can simply “speak” the computer language with the API and obtain all the information they need.

Mobile apps, websites and even desktop applications regularly rely on third-party data or functionalities that they consume through web APIs. Web APIs provide applications with otherwise inaccessible resources, such as access to global social networks (examples: web APIs provided by Twitter, Facebook or LinkedIn), advanced machine learning capabilities (examples: web APIs provided by IBM Watson or Google Cloud’s AI) or complex transaction processing (examples: web APIs by Stripe or PayPal for payment processing or the Flight Booking API).

Although most companies are well-versed as to where their web applications reside, they may have little to no visibility into the full complement of APIs on which their businesses depend.

In other words, application developers now rely heavily on third parties — entities beyond their control sphere — for core functionality of their applications. User experience and, by extension, application reputation are directly affected by actions and nonactions of the API provider(s). Service-level agreements (SLAs) might come

into play for commercial API offerings, but by and large, developers are no longer in control of their apps. And APIs make it much more difficult to distinguish good bots from bad bots.

APIs UNDER SIEGE

Scammers exploit API vulnerabilities to steal sensitive data, including user information and business-critical content. Modern application architecture trends — such as mobile devices, use of cloud systems and microservice design patterns — complicate security of APIs because they involve multiple gateways to facilitate interoperability among diverse web applications. What’s more, extensive deployment of internal APIs, combined with mobile access and increased dependence on cloud-based APIs, means that web application security defense systems that defend only the external perimeter are ineffective. Also, as businesses continually add and consume new APIs, API security cannot be a one-time exercise.

Following is a roundup of the most common bot attacks against APIs:

Application DDoS Attacks

Attackers overwhelm APIs by sending traffic from multiple clients. They target business-critical services, including login services, session management and other services vital to application reliability. Attackers also generate API calls that require extensive resources and affect server response time. Detecting and filtering unwanted traffic, including requests from automation scripts, are essential for stopping DDoS attacks on Layer 7. The key is analyzing every API request, including payload and HTTP headers, to identify anomalous behavior patterns and performing intent analysis to understand the actual intent behind an API request to filter bad API calls.



Account Takeover

Hackers deploy botnets to programmatically send API calls to test stolen credentials. Although API management systems reject invalid login attempts, these systems are incapable of stopping bot herders from trying different combinations of credentials using multiple IPs. Hackers also keep the API requests below the rate limit to make it difficult for conventional API security measures to detect such sophisticated account takeover attempts. It is important to accurately distinguish between genuine login attempts and malicious credential stuffing attacks.

Web Scraping

Scrapers extract data from APIs and execute automated form filling. Hackers reverse-engineer web and mobile apps to hijack API calls and scrape content.

MOBILE APPS

With the ubiquitous adoption of the mobile internet, cyberattackers have found yet another attack surface to exploit. Attackers target mobile apps to prey on business-critical data, customers' personal information, credentials and payment card details. These bots change their identity, behavior and IP address to operate under permissible limits of conventional security measures. Additionally, mobile traffic characteristics are less predictable than web browsers' traffic. Tackling such sophisticated bots requires an advanced approach that improves its logic faster than continuously evolving bot patterns.

Hackers abuse mobile apps by creating virtual machines – that is, virtualizing a smartphone, running the app on that virtual machine and then duplicating it 1,000 times or more. It's a perfect formula for committing click fraud using

a legitimate mobile app. And hackers can usually get away with it unless and until the app developer implements a capability to detect whether the app is running on an iPhone or Android device or in a virtual machine environment.

More advanced hackers take the tactics to another level – reverse-engineering a mobile app to reuse the API calls it makes and placing those within their own app. This raises the need for app owners to distinguish the source of calls against their APIs. And it requires the ability to verify where the app is compiled. If it hasn't been compiled in a safe and approved environment, those API calls should be ignored.

WEBSITES

Bad bot tools are a dime a dozen – making it relatively easy for attackers to acquire the resources they need to spam, scrape, scalp or otherwise abuse your website. Web scraping has emerged as one of the predominant uses for bots. Programs that execute these content-stealing attacks are as diverse as they are popular, ranging from simple, manually tuned scripts to highly automated, cloud-based services. Other tools serve in a supporting role.

This piece, [*The Top Free and Paid Web Scraping Tools and Services*](#), provides an overview of the top web scraping tools, cloud-based services and IP rotation solutions currently used to conduct web scraping attacks.

READ
[THE TOP](#)
[FREE](#)
[AND PAID](#)
[WEB](#)
[SCRAPING](#)
[TOOLS AND](#)
[SERVICES](#)

4.0

Detection & Mitigation Techniques

WHEN IT COMES TO DETECTION AND MITIGATION, SECURITY AND MEDICAL TREATMENT HAVE MORE IN COMMON THAN YOU MIGHT THINK. BOTH REQUIRE CAREFUL EVALUATION OF THE RISKS, TRADE-OFFS AND IMPLICATIONS OF FALSE POSITIVES AND FALSE NEGATIVES.

You may be able to see a higher-than-usual volume of bot traffic, but that doesn't reveal bot intent or risk factors.

In medicine as well as security, detecting a problem is not the same as detecting *the* problem. For example, although it's easy to identify a high fever, the presence of a fever does not clearly indicate a certain disease and, by extension, a course of treatment. The same holds true when diagnosing bot activity. You may be able to see a higher-than-usual volume of bot traffic, but that doesn't reveal bot intent or risk factors.

In both disciplines, it's critical to use the right treatment or tool for the problem at hand. Taking antibiotics when you have a viral infection can introduce unwanted side effects and does nothing to resolve your illness. Similarly, using CAPTCHA isn't a cure-all for every bot attack. It simply won't work for some bot types, and if you deploy it broadly, it's sure to cause negative customer experience "side effects."

And in both medicine and security, treatment is rarely a one-size-fits-all exercise. Treating or mitigating a problem is an entirely different exercise from diagnosing or detecting it. Figuring out the "disease" at hand may be long and

complex, but effective mitigation can be surprisingly simple. It depends on several variables — and requires expert knowledge, skills and judgment.

Medicine is increasingly moving to a "personalized" approach based on a patient's specific genetic and lifestyle variables. In the realm of bot management, security needs to do the same. Every business is running a distinct set of websites, applications and mobile apps and relies on a unique set of APIs. And each has different priorities and levels of comfort with false positives and false negatives.

The only way to meet those nuanced requirements is with a tailored approach that leverages machine learning to continually monitor the "genetics" of your business, the environment in which it operates and the attackers seeking to harm it.

A closer look at bot detection and mitigation will explain why.

DETECTION





On the surface, bot detection seems simple: You want to accurately detect bad bots with a low rate of false positives (to avoid blocking legitimate human users and good bots) and a low rate of false negatives (to ensure that you're detecting ALL bad bots). Go below the surface though, and the challenges of detection become much more complex.

There's a good reason why analyst firm Forrester has cited attack detection as one of the major selection considerations for bot management

solutions.²⁵ The quality of detection determines the quality of the solution. And as attacking bots become ever more sophisticated, detection becomes ever more challenging.

Chapter 2 presented the four generations of bots, highlighting the increasing levels of sophistication over time. For simpler bots, the detection process will be comparatively fast, easy and inexpensive. However, as bots become more sophisticated, detection will become longer, more challenging and more costly (see Figure 13).

FIGURE 13. MITIGATION OPTIONS BY BOT GENERATION

				
GENERATIONS	FIRST GENERATION IP and HTTP reader combinations	SECOND GENERATION Device fingerprints: format checks, logical checks across attributes, reputation database	THIRD GENERATION Shallow machine learning	FOURTH GENERATION Deep machine learning
BOTS	SCRIPT BOT	HEADLESS BROWSER BOT	HUMANLIKE BOT	DISTRIBUTED BOT
TECHNOLOGY	BLACKLISTS IP, UA	DEVICE/BROWSER Cookie, JS, fingerprinting	INTERACTION (SHALLOW) Mouse movement & keystroke anomalies <small>└── User Behavioral Analysis ─┘</small>	INTENT (DEEP) Correlation in intent signatures across devices

To illustrate these points, consider the example of a bot attack aimed at cracking passwords. A bot management solution could apply several methodologies to detect the attack by:

1. Identifying the average activity rates and abnormal rates of unsuccessful login attempts. Unfortunately, this approach is not sufficiently accurate and, more important, does not identify the attack source. Thus, any mitigation will be ineffective or will have a significant customer experience impact.
2. Looking at each source IP address and correlating activity over time to allow detection of active IPs generating unsuccessful login attempts. However, if the attack source is dynamically rotating its IP addresses, this methodology will be blind to the attack.
3. Correlating the activity over time for each source by device fingerprint. But again, if the attack source is dynamically modifying its device fingerprint, the methodology will miss the mark.

A more sophisticated detection will correlate activity over time across IPs, device fingerprints, mobile device attributes and sensors, as well as other attributes, to provide comprehensive analysis for accurate attack source detection.

²⁵The Forrester New Wave: Bot Management, Q3 2018

MITIGATION

Blocking bots may seem like the obvious approach to mitigation; however, mitigation isn't always about eradicating bots. Instead, you can focus on managing them. What follows is a round of mitigation techniques worth consideration:

1. Feed fake data to the bot. Keep the bot active and allow it to continue attempting to attack your app. But rather than replying with real content, reply with fake data. You could reply with modified faked values (that is, wrong pricing values). In this way, you manipulate the bot to receive the value you want rather than the real price. Another option is to redirect the bot to a similar fake app, where content is reduced and simplified and the bot is unable to access your original content.

"It's easy to embed a CAPTCHA into my apps. Why would I need a bot manager?"

Not so fast. Whom should you challenge with your CAPTCHA? How do you identify your attacker? Do you really want to challenge everyone?

You can't know how to deploy CAPTCHA without effective detection. Without it, either you'd be challenging the wrong attackers or you would be challenging everyone — impacting visibility and user experience.

2. Challenge the bot with a visible CAPTCHA. CAPTCHA can function as an effective mitigation tool in some scenarios, but you must use it carefully. If detection is not effective and accurate, the use of CAPTCHA could have a significant usability impact. Since CAPTCHA is a challenge by nature, it may also help improve the quality of detection. After all, clients who resolve a CAPTCHA are more than likely not bots. On the other hand, sophisticated bots may be able to resolve CAPTCHA. Consequently, it is not a bulletproof solution.

3. Use throttling. When an attack source is persistently attacking your apps, a throttling approach may be effective while still allowing legit sources access to the application in a scenario of false positives.

4. Implement an invisible challenge. Invisible challenges can involve an expectation to move the mouse or type data in mandatory form fields — actions that a bot would be unable to complete.

5. Block the source. When a source is being blocked, there's no need to process its traffic, no need to apply protection rules and no logs to store. Considering that bots can generate more than 90% of traffic for highly attacked targets and applications, this cost savings may be significant. Thus, this approach may appear to be the most effective and cost-efficient approach. The bad news? A persistent attack source that updates its bot code frequently may find this mitigation easy to identify and overcome. It will simply update the bot code immediately, and in this way, a simple first-generation bot can evolve into a more sophisticated bot that will be challenging to detect and block in future attack phases.

A HEALTHY BOT MANAGEMENT STRATEGY

Here's an overview of the basic functionality you need to mitigate — or manage — bots:

1. A session is a single context from a single user or client accessing your app. A bot manager must add a cookie in the web environment or a token in the API environment in order to monitor and analyze session context.

2. A bot manager must correlate all the behaviors of all sources across all sessions for the purpose of attack detection. Those behaviors should include volume, nature, frequency of transactions and navigation flow.

3. A bot manager should be able to uniquely identify sources. Consider the simple example of an attacker trying to crack a particular user's password. Suppose it tries three times to log in with a dictionary password before switching to another IP. In such a scenario, IP-based identification of the attack source is ineffective, and you're blind to the attack.

To correlate across those multiple attack attempts, you need a device fingerprint to gather IP-agnostic information. Even if the same attack source uses a dictionary of the 1,000 most common passwords and keeps switching IP addresses, you need the ability to identify the behavior and the context over multiple sessions. To do so requires you to embed device fingerprint JavaScript into the secured application or into the application responses. In other words, there is a need to modify the response if JavaScript is not embedded into the application.

Finally, while device fingerprinting is effective in a web environment, a mobile device that may not execute JavaScript requires a different approach. In that case, you need a collection of mobile device sensor data for source identification. By integrating the application with a mobile software development kit (SDK), you can enable access to mobile device sensor data.



IMPLEMENTATION OPTIONS

API ENDPOINT	SPAN PORT	IN-LINE
<p>The data path component has visibility into the application traffic, while the actual analysis of the traffic is applied in a centralized cloud/on-premise API endpoint component.</p> <p>Mitigation may be applied in the same data path component or elsewhere.</p>	<p>A concept available on every switch that allows you to take a copy of the traffic being sent from client to web server and back to client.</p> <p>Although you can't modify the traffic (request or response), you do see them and can collect this information for complete analysis without impacting data latency or response times.</p>	<p>Delivered as a reverse proxy or as a bridge.</p>
<p>ADVANTAGES: Reduced data path risk allowing controlled latency with configurable timeout, no point of failure with bypass options and an option to implement an asynchronous approach.</p>	<p>ADVANTAGE: Zero impact to traffic.</p>	<p>ADVANTAGES: Allows inspection before forwarding the request to the secured application.</p> <p>Allows response modification for embedding JavaScript.</p>
<p>DISADVANTAGES: None</p>	<p>DISADVANTAGES: No response modification and limited detection capabilities.</p> <p>Just visibility – NOT mitigation.</p> <p>While some organizations prioritize visibility into the problem over mitigating it, this approach isn't practical for bot management solutions.</p>	<p>DISADVANTAGES: May introduce latency and point of failure.</p>

4. A bot manager also needs to offer a rules engine with deterministic rules that support immediate attack detection and mitigation.

5. Finally, a bot manager needs machine learning capabilities to detect sophisticated bots whose behavior cannot be detected by deterministic rules. A legitimate behavior for one app may be completely illegitimate in a different app and allow bot activity detection.

DEPLOYMENT OPTIONS

Although a bot management service may offer cloud control and one centralized, multitenant portal, the primary provisioning/deployment option for data path integration should be reviewed.

Following are the three options:

1. Cloud integrated. Various vendors offer cloud-integrated bot services that require redirection of client traffic, so the bot manager can process all traffic for bot detection. The common approach is domain name system (DNS) redirection. Such services are offered by cloud web application firewall (WAF) integrated bot management service providers and by content delivery network (CDN) service providers.

2. Application integrated. With this deployment option, there is no redirection of traffic to a cloud data path service. The data path visibility, detection and mitigation component may be integrated in:

- A reverse proxy, such as Envoy, NGINX or HAProxy, which is usually implemented as a plug-in or a module integrated into the reverse proxy or as a script implementing the bot management functionality
- The web server running the application where a plug-in implements the bot management functionality
- The web application itself using SDK integration
- The mobile app using mobile SDK integration

3. Appliance. Usually an appliance implementation will be based on a prepackaged reverse proxy option (described above) delivered as a physical or virtual appliance.



5.0

Additional Considerations

WAF OR BOT MANAGEMENT?

WAFs ARE PRIMARILY CREATED TO SAFEGUARD WEBSITES AGAINST APPLICATION VULNERABILITY EXPLOITATIONS. WAFs USUALLY FEATURE BASIC BOT MITIGATION CAPABILITIES AND CAN BLOCK THOSE BASED ON IPs (THAT IS, ACCESS CONTROL LISTS OR ACLs). IF THE WAF IS A BIT MORE SOPHISTICATED, IT MAY ALSO BE ABLE TO PERFORM DEVICE FINGERPRINTING.

However, WAFs fall short when faced with some automated threats (example: content scraping). Moreover, fourth-generation bots use sophisticated techniques to evade detection — from mimicking human behavior and abusing open-source tools to making multiple violations in different sessions.

When it comes to detecting and mitigating fourth-generation bots, WAFs simply don't do the job well enough.

Two to Tango

Complete application protection must bring together the ability to detect and control malicious bot attacks as well as to secure the “by-design” flaws. In many cases, bots are programmed to exploit these vulnerabilities, but again, they can do a lot more.



SCANNING...

WHEN DO WAFs DO THE JOB? WHEN DO YOU ALSO NEED TO BRING IN A BOT MANAGER?

The table below provides an at-a-glance view of each one’s strengths – and in what cases they play well together:

SECURITY CAPABILITIES	BOT MANAGER	TRADITIONAL WAFs	HAVING BOTH
Protection from simple bots	YES	YES	YES
Fingerprinting malicious devices	YES	YES	YES
Mitigation of dynamic IP and headless browser attacks	YES	LIMITED	YES
Detection of sophisticated bot attacks	YES	NO	YES
Risk of blocking genuine users (false positives)	NONE	HIGH	NONE
Collective bot intelligence (for example, IPs, fingerprints and behavioral patterns)	YES	NO	YES
Customized actions against suspicious bot types	YES	NO	YES
Protection from OWASP Top 10 vulnerabilities	NO	YES	YES
Protection from API vulnerabilities	LIMITED	YES	YES
Protection against Layer 7 DoS	LIMITED	YES	YES
HTTP traffic inspection	NO	YES	YES
Masking sensitive data	NO	YES	YES
Compliance with HIPAA and PCI	LIMITED	YES	YES
Integration with DevOps	NO	YES	YES



6.0

Buyers Checklist

KEY CONSIDERATIONS WHEN EVALUATING BOT MANAGEMENT SOLUTIONS
WE'VE SUMMARIZED THE CHALLENGES. WE'VE OUTLINED OPTIONS FOR DETECTING AND MITIGATING BOT ATTACKS. THIS CHAPTER EXPLORES KEY CONSIDERATIONS WHEN EVALUATING BOT MANAGEMENT SOLUTIONS. USE THESE CRITERIA TO SELECT THE BEST SOLUTION FOR YOUR ENVIRONMENT.

CONSIDERATION #1: SCOPE OF DETECTION TECHNIQUES

The rise of highly sophisticated, humanlike bots requires advanced techniques in detection and response.

Ask the following:

- What detection and response techniques does the solution support?
- How many methodologies are included, and what is their level of sophistication?

For the most advanced capabilities, look for a solution that offers a full complement of techniques, including device and browser fingerprinting, intent and behavioral analyses, collective bot intelligence and threat research, as well as other foundational techniques.

CONSIDERATION #2: ADAPTABILITY TO DYNAMIC THREATS

Bots never stop evolving. Neither should your bot management solution.

Ask the following:

- Does the solution include deep learning and self-optimizing capabilities? These capabilities are essential for identifying and blocking bots as they alter characteristics to evade detection.
- Does the solution match the deception capabilities of sophisticated bots? Request examples of sophisticated attacks that the solution has successfully detected and thwarted.

CONSIDERATION #3: MULTIGENERATIONAL DETECTION

Each of the four current bot generations requires different approaches to mitigation.

Ask the following:

- How does the solution defeat earlier generations? Techniques such as blacklists, fingerprinting and JavaScript are the most common approaches.
- How does the solution take on modern bots, which extend their capabilities beyond scripts and headless browsers? Humanlike bots and advanced distributed bots require complex user behavioral analysis.
- How does the solution understand and neutralize a bot's intent?



SCANNING...

CONSIDERATION #4: ROBUST AUTOMATED RESPONSE

It's important to choose a solution that offers multiple response mechanisms to bot traffic.

Ask the following:

- Does the solution include not only blocking but also limiting custom actions based on threat identification?
- Can it serve fake data to the bot?

CONSIDERATION #5: DEPLOYMENT FLEXIBILITY

Every network is different.

Ask the following:

- How well does the solution accommodate your network's unique needs?
- Can the provider deploy the solution exactly the way you need it? Look for a bot management solution that provides easy, seamless deployment without infrastructure changes or the risk of rerouting traffic.
- Does your architecture require an in-line solution or something out-of-path?
- Do you want it to detect and mitigate or only to detect and notify?

Be sure to look for options that can be stand-alone or integrated with a WAF for complete coverage.

CONSIDERATION #6: CLEAN, FEATURE-RICH REPORTING FOR OPTIMAL VISIBILITY

Reporting is a critical aspect of any bot management tool. Consider how each solution provides reporting information. Having access to granular reports can be crucial, yet too much information can also hide what you're looking for.

Ask the following:

- Does it offer clean, easy-to-understand reporting? It should present granular detail when you want it to but also integrate with popular analytics platforms from Adobe or Google to provide reports on nonhuman traffic.

CONSIDERATION #7: GOVERNANCE AND COMPLIANCE FACTORS

For many organizations, their applications and supporting data are among their most valued assets.

- Does the bot mitigation solution ensure that traffic does not leave a network?
- If so, does it transform data to an encrypted and hashed format to maximize privacy and compliance?

Ensuring that the bot mitigation solution is compliant with the General Data Protection Regulation (GDPR) pertaining to data at rest and data in transit will help to avoid personal data breaches and the risk of financial and legal penalties.

**FOR MORE
DETAILS ON
THIS TOPIC,
SEE THE
RADWARE
WHITE PAPER
HOW TO
EVALUATE BOT
MANAGEMENT
SOLUTIONS.**

CLOSING

IN AN IDEAL SECURITY WORLD, IT WOULD BE EASY TO IDENTIFY GOOD BOTS VS. BAD BOTS. WE WOULD SIMPLY ENABLE HELPFUL BOTS AND BLOCK THEIR HARMFUL COUNTERPARTS. AS WITH MANY ASPECTS OF TECHNOLOGY MANAGEMENT — AND DAY-TO-DAY LIFE — THE REALITY IS FAR MORE NUANCED. SIMPLISTIC APPROACHES MAY HELP THWART BAD BOTS, BUT THE PRICE WILL BE TOO HIGH IN TERMS OF LOST BENEFITS FROM GOOD BOTS — NOT TO MENTION CUSTOMER FRUSTRATION AND DISENFRANCHISEMENT.

Ultimately, your goal should not be to eradicate bots but rather to manage them effectively. By using mitigation and detection techniques that are sophisticated and continually refined, you can ensure that your organization enjoys bot benefits while reducing the impact of bad actors.



SCANNING...

APPENDIX

OWASP TOP 21 AUTOMATED THREATS

ACCOUNT TAKEOVER

CREDENTIAL CRACKING
CREDENTIAL STUFFING
ACCOUNT CREATION
ACCOUNT AGGREGATION
TOKEN CRACKING

AVAILABILITY OF INVENTORY

DENIAL OF INVENTORY
SCALPING
SNIPING

ABUSE OF FUNCTIONALITY

DATA SCRAPING
SKEWING
SPAMMING
CAPTCHA DEFEAT
AD FRAUD
EXPEDITING

PAYMENT DATA ABUSE

CARDING
CARD CRACKING
CASHING OUT

VULNERABILITY IDENTIFICATION

FINGERPRINTING
FOOTPRINTING
VULNERABILITY SCANNING

RESOURCE DEPLETION

DENIAL OF SERVICE

[HOW TO EVALUATE
BOT MANAGEMENT
SOLUTIONS](#)

[THE TOP FREE
AND PAID WEB
SCRAPING TOOLS
AND SERVICES](#)

[THE 50 MOST
COMMON WEB
SCRAPING TOOLS](#)

CONTACT US
[ABOUT BOT
MANAGEMENT
SOLUTIONS](#)

**FOR MORE
INFORMATION**
[VISIT OUR BOT
MANAGEMENT
RESOURCE
CENTER](#)

ABOUT RADWARE

Radware® (NASDAQ: RDWR), a leading provider of cyber security and application delivery solutions, acquired ShieldSquare in March 2019.

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.

© 2021 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are property of their respective owners.

