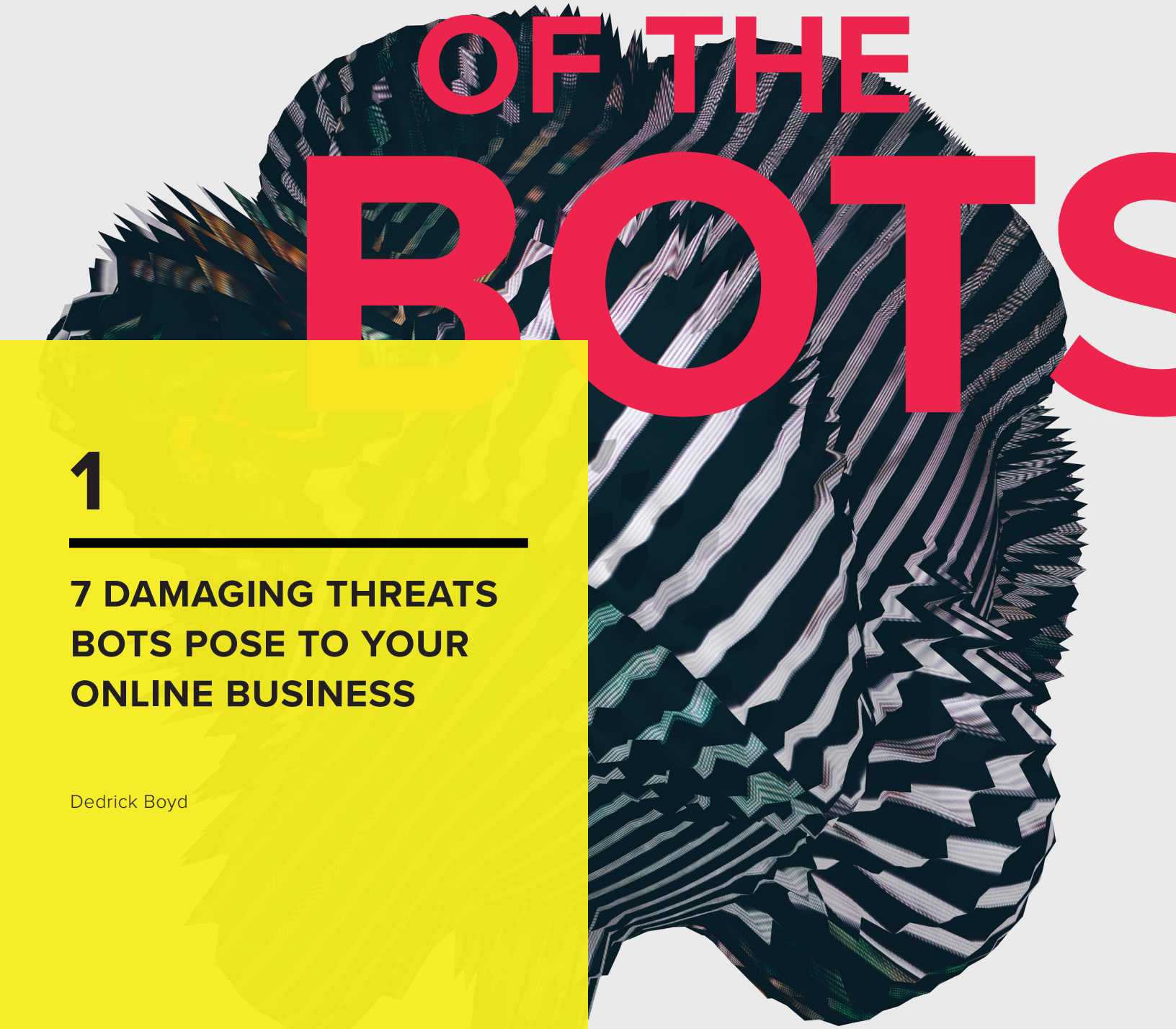
RISE OF THE BOTS



1

7 DAMAGING THREATS BOTS POSE TO YOUR ONLINE BUSINESS

Dedrick Boyd

TECHSPARQ

techsparq.com

"IT'S NOT A MATTER OF IF, BUT WHEN YOU WILL BE ATTACKED."

Troy Leach,
CTO of Payment Card Industry Security Standards Council

BOTS ARE LEVERAGING TECHNOLOGY TO DISRUPT RETAILERS

Bots have become an unavoidable part of online commerce for shoe and apparel retailers of any size from large-scale operations like Nike and Adidas to specialty operations such as End and Supreme. A bot is a software application that performs automated tasks (scripts) such as appointment reminders, dinner reservations, or online searches. Bots perform tasks that are simple and structurally repetitive much faster than a human would on their own.

Bots are everywhere on the internet. Good bots can inlcude lead generation, customer service, chatbots, and search engine spiders. Chat bots can reduce costs by assisting companies in research. Search engine spiders crawl the internet while indexing information. Malicious bots can coordinate denial of service attacks (DDoS) or interfere with your e-commerce site.

However, company-created bots that automate repetitive human tasks can create significant cost savings, as well as, aid in developing new streams of revenue.

THE FINANCIAL CONSEQUENCES OF MALICIOUS HACKERS AND BOTS ARE SIGNIFICANT

The shift away from brick and mortar stores to e-commerce has been seismic. As retailers are in near-constant flux adjusting their businesses and processes to the ever-changing consumer, they must also adjust their business processes and utilize technology to thwart hackers and their tools as they continually look for system vulnerabilities to exploit.

The financial consequences of malicious hackers and bots cannot be overstated. Businesses, even huge retailers with solid infrastructure, have been crippled by little more than a guy and a laptop. How might these hackers target your business?

01 Account Takeover

Account takeover relies either on a brute force approach, trying many combinations of usernames and passwords on a popular login page or on stolen login combinations. The bad news is the brute force method is astoundingly successful. This is in large part because many users choose passwords that are foolishly obvious.

PerimterX studied a brute force attack that had an incredibly high success rate of 8%

This bot attack tried 5 million combinations per day, which suggests it broke into about 400,000 accounts daily. Once an account was taken over, the hacker had instant access to any stored credit card data and personal information of the real account owner.

02 Fake User Creation

Fake user creation may not sound nefarious but it can be devastating. Minor consequences can include lost revenue when a fake account is used by a person to collect a discount code or to get another thirty days of free movie streaming. Hackers use this on an entirely different scale by amassing millions of fake users, effectively giving them control over a large army of registered (though fake) users on your website.

One danger is DDoS via hoarding. For example, a hacker with thousands of what looks like legitimate users reserves all of the cars that a particular rental car company has in a given city, but never ultimately rents the vehicles. This causes massive disruption, confusion and lost revenue.

03 Carding

Carding, or theft of gift card balances, is a significant problem. Attackers understand the number structure of gift cards and may try many millions of combinations to break into a gift card account to steal the balance.

With 93% of Americans giving or receiving a gift card every year, there is plenty of rich, low-hanging fruit here for thieves. This erodes customer confidence in both the brand and the brand's ability to secure personal information.

04 Marketing Fraud

Marketing fraud poses a serious threat to e-commerce and media businesses. Ever since companies began paying for clicks and traffic, criminals have had a motive to generate bogus traffic, so they can charge for the clicks and traffic. Marketing fraud has existed since the late 1990s but has evolved significantly.

The bottom line is that bots leverage technology and existing business processes to target businesses in ways both good and bad.

05 Content Theft

Content theft often takes the form of scraping. If you own a commerce site, your competitors want your pricing, your current inventory, and your SEO-optimized product descriptions. If you own a news outlet or media content site, hackers want to steal your proprietary and confidential content to post it on third-party sites as their own.

This content theft can put you at a competitive disadvantage and dilute the optimization and ranking of original content you paid to have created. This wastes your marketing dollars and dulls your competitive edge.

06 Checkout Abuse

Checkout abuse is what happens when you try to buy a high-demand product online like the latest Air Jordan sneaker or Taylor Swift concert tickets. As you know, it's nearly impossible to get these highly sought-after items. Within minutes, all of the inventory is gone. Bots are behind almost all of these near-instant purchases. The perpetrators hoard and then resell their inventory on the secondary market for huge profits.

The bots create a scarcity by hoarding products and then exploit the scarcity by scalping. The perpetrators make a huge profit on your products whether they're sneakers on Ebay or heavily marked up concert tickets on StubHub. This distortion of the efficient, natural marketplace causes problems for both retailers and consumers. For the retailer, it damages consumer trust and business profitability over the long term.

07 Inflated Traffic

Inflated traffic happens when bad bots visit your site and are designed to disrupt your business either for financial gain, competitive advantage, or simply because they can.

Their methods are also becoming more and more complex and resistant to detection. It is estimated that over 21% of typical traffic on an e-commerce site is actually driven by bots. That volume of illegitimate traffic means that most current e-commerce sites are hugely overbuilt. They don't need the computing power they are currently using for legitimate traffic. Instead, they are accommodating a huge chunk of traffic that contributes zero to their bottom line. In fact, the retailer is paying to lay the pathways for hackers and bots to disrupt their business. This drives up the cost of doing business and the huge flow of traffic also makes it harder to find the bad actors.

in 2019 Bad Bots Accounted for the following:

$5.8 BILLION
IN AD-RELATED FRAUD

Source: Association of National Advertisers

70%
INCREASE IN BOT ACCOUNT REGISTRATION FRAUD

Source: Arkose Labs

+21%
BAD BOTS E-COMMERCE WEB TRAFFIC

Source: Distil Networks

The Four Generations of Bots

As the Web has evolved, we have witnessed evolution of bots and automation engines. We can identify four distinct generations of bots. Generation 4, the newest, is an actual browser running on a device that belongs to an acutal - and presumably innocent - user, exploiting that user's device, credentials and environment.

451 Research has labeled the behavioral based approach of detecting and blocking bots "Web Behavior Analytics" (WBA).

It is the cornerstone of bot defense.

GETTING & STAYING AHEAD IN THE BOT RACE

Vulnerability to bots is, and should be, a major concern for any company doing business online, especially retailers. Though the threat is real and the risks high, technology and innovation continue to keep pace. Basically, criminals build a better bot and then we build better defenses. It can be exhausting and costly to keep up with the ever-present threat of bots, DDoS attacks and more, but it must simply become a known part and cost of doing business online. E-commerce is a huge source or opportunity for revenue. This must be maximized and protected.

Get a Handle on Bot Activity on Your Site

Working around bots to get highly sought-after products into the hands of consumers is certainly one way to stop hoarding and other bot issues. However, the first important step is to have a firm grasp of bot activity on your e-commerce site. Bots and automated web attacks are continually evolving as companies work to shore up against them. The newest iterations of bots are becoming seriously good at operating under cover as legitimate users. To know whether you are dealing with a bot or not, you must understand the behavior of your users.

Instead of simply trying to protect data and service endpoints, the logical next step must be to analyze what's occurring on the website. Tech innovation is identifying and solving these problems with behavior-based analysis and machine learning.

Human behavior is pretty hard to mimic: our actions are a bit random, erratic even. Coding, by its nature, is systemizing, so automating actions to happen faster and more consistently than human interaction on your site occurs naturally.

But writing code to mimic actual human activity is difficult. Most programs behave in a linear, systematic fashion. Sure, some variance can be programmed so that each button click does not occur at a speed at which no human could ever operate, but there are a number of metrics like how the mouse is moved and how scrolling occurs and more that are harder for bot creators to disguise. These can be analyzed to distinguish between bots and human users by using next generation behavior-based analytics.

Hackers Attack Your Most Vulnerable Areas

Hackers look beyond the typical areas and methods of attack. They set their sights on areas between technology, security, and business operations that are less scrutinized, where bot attackers can go undetected longer. Quite often, the hackers will target a company's web applications and business processes to expose the company to a wide array of risks. As business processes become more exploited, it's essential to add additional safeguards.

For example, if the forgotten password functionality is used, followed by an email address change, and then a physical address change, should the e-commerce site validate these changes before allowing the customer to place a new order?

A real user will understand that making all of those changes in a rapid succession might arouse suspicions so they will take the extra step to validate their identity. However, a bot could get "stuck" at this challenge step. Or it may not be able to place a phone call to the retailer, provide the code displayed on the screen or do whatever action is required to verify the changes. This safeguards both the retailer and legitimate users.

Is Your Site Capable of Handling the Added Load Bots Push?

While not all bots are hostile, they can still be disruptive because they add an extra load your site must be able to handle. With activity from consumers, hostile bots and friendly but active bots, you can get thousands of login attempts every second.

Web application firewalls (WAFs) have been the gold of security for years. However, they do nothing to protect business logic from bot abuse.

Areas of focus to get ahead in the Bot Race:

One/ Work around bots and find different ways to get hot products to consumers. Two/ Identify bot activity like hoarding and shut it down. Three/ Defend against bots by shoring up e-commerce sites to handle the added load bots push. Four/ Work with pseudo-friendly bots to keep them in their lane.

Keep Bots Firmly in Their Lane

While no one likes the idea of bot activity on their e-commerce site, there are consumer-driven bots that can help drive revenue if managed in a way that restricts them from interfering with your consumer web traffic. From conversational selling bots to chat bots to APIs, done correctly, bots can provide as many opportunities as they do headaches.

For example, sneaker/apparel retailers are starting to use chatbots, powered by machine learning and natural language processing, to provide customers with fine-tuned service, sales and support.

Whether your business is looking to cut costs by transferring previously human-supported services to bots or looking for an affordable way to promote more brand-to-consumer interaction, bots and APIs are providing cutting-edge possibilities.

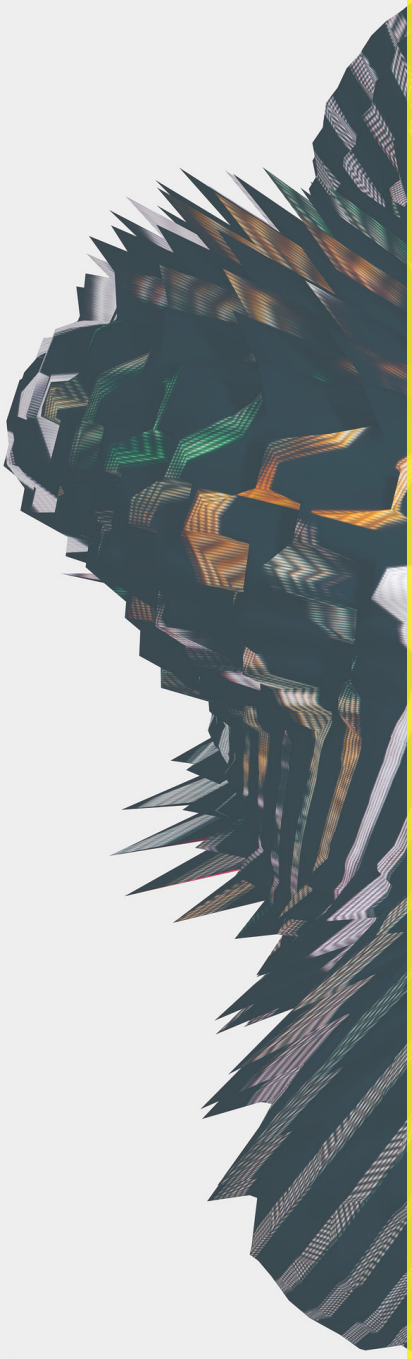
Chat bots and conversational commerce offer the chance to create a sense of connection without people and are rapidly changing the future of customer support.

HOW TECHSPARQ CAN HELP IDENTIFY THREATS & OPPORTUNITIES

Technology is changing the sportswear and apparel industry at record speed. At TechSparq, we work exclusively within the retail industry to help companies identify threats and maximize opportunities. We understand the bot landscape, the possible implications on your e-commerce business, and your bottom line.

With our industry knowledge, deep technical skills and agile approach, we can evaluate your current systems and processes to determine what threats are looming, how to continually mitigate them and how your company could be using bots to reduce cost and increase customer satisfaction.

To find out more about how TechSparq can reduce risk and smooth your company's path to the future:
www.techsparq.com or 1-800-640-5589.



About TechSparq

Techsparq is a leading provider of software solutions for retail technology. For 12 years we've been delivering software solutions, process improvement and cost savings to our clients. We provide expertise to tackle technological business challenges in any economic climate.

For more information: *www.techsparq.com*

About the Author

Dedrick Boyd has over 20 years of experience in the software and package implementation space from custom software, application integration, enterprise integration, implementation strategy, project management, to e-commerce implementation. He is performance-driven with expertise in developing and executing strategic e-commerce roadmaps aimed at increasing sales & profit, solidifying system resilience/stability/performance, and improving customer experience and loyalty. Dedrick has helped to modernize software, implement strategy, and drive customer loyalty for industry leaders like Nike, Columbia Sportswear, Home Depot, Walt Disney Company, Target, Mattel, Unilever, and more.

TECHSPARQ

Locations

Portland, OR
Atlanta, GA

Contact

800.640.5589
info@techsparq.com