Dan Ross
Comp 116
Professor Chow
May 7, 2018

Sneakerbots: The Tyrants of Ecommerce

ABSTRACT:

Sneakerbots are programs that automate the sneaker purchasing process. As the second hand market for sneakers developed, sneakerbots also grew and became more popular and advanced. Sneaker-heads (sneaker collectors) compete with individuals looking to flip the sneakers for large profits, so both use bots to get the best chance of obtaining the shoes. However, retailers do not support these unfair practices and look for ways in which they can ban bots, or develop checkout processes that never allow for bot interference at all. This paper examines the ways in which sneaker companies combat bots, and suggests that these practices shed valuable insight into how to combat the larger bot attacks that plague ecommerce as a whole.

INTRODUCTION:

In February 2005, for four days nearly 100 people camped out during a New York City Nor'easter for a chance to purchase a sneaker. The Nike SB "Pigeon" dunk was a limited edition collaboration between Nike and Jeff Staple, owner of the Reed Space boutique, and today is credited as "the shoe that catapulted sneaker culture to the masses." Within the sneaker community the prelude to the release is as infamous as the sneaker itself, as police tried to force those camping out for the shoes to return home resulting in riots fought with baseball bats and machetes. The release even gained national traction as CNN covered the event.[1] As sneaker culture grew, so did the Internet, and by 2011 retailers looked to ecommerce to control often-chaotic releases.

While the Internet offered an opportunity for sneaker retailers to avoid the physical mayhem witnessed during the "Pigeon" dunk release; moving to the web without considering the potential online sales exploits proved more unjust to the customer than allowing the occasionally dangerous lineup outside a shop. For many, their local sneaker shop was a unique opportunity to purchase coveted shoes, but as retailers went online, suddenly people across the globe were trying to purchase the shoes rather than the neighborhood sneaker-heads. Retailers were not blind to the overwhelming demand either, before 2011 sneaker giants like Nike and Adidas tried to release sneakers online yet the high traffic led to servers crashing, sites going down, and unfulfilled orders. However, in 2011, Kith, a popular New York City sneaker boutique, collaborated with Shopify, and started to produce online releases that could handle the intense "flash sale conditions".[2] Without being able to physically beat out someone by getting inline earlier than the next person, customers experimented with software to gain an advantage over their competition.

Today, online sneaker releases are plagued by sneaker-bots, software that automates purchasing sneakers. With sneaker-heads competing with individuals looking to profit off limited releases, it is no surprise bots became so popular. Nonetheless, bots give these individuals a serious advantage and too often the limited shoes end up in the same hands over and over, regardless of whether the customer is a sneaker-head or not. Now, the sneaker community is faced with the opportunity to employ more advanced technologies such as biometric authentication and augmented reality, to not only defeat bots in the sneaker world, but also impact the larger fight against the bots that torment ecommerce.

TO THE COMMUNITY:

The sneaker industry is home to some of the largest companies in the world; it has both the global reach and resources to stop bots from creating an unfair online marketplace. For example, Nike sits in the top 100 largest global companies.[3] Nike's messages are heard and projected across the globe, and if they allow customers to use bots to purchase their shoes, they send a message that they support unfair commerce. Fortunately, Nike is a leader in the combat against bots, and works diligently to create a system that makes it difficult for bots to penetrate their buying experience. [4] However, smaller businesses that attempt to produce fair shopping experiences with "first come, first-served" tactics too often fail. Highsnobiety writer Chris Danforth said, "The fact of the matter is: the problem is only likely to become worse. Any e-commerce framework that operates on a "first come, first-served" basis is a perfect target for bots, as computers are indisputably faster than humans at clicking."[5] Shops cannot trust users that they are honestly clicking through their site and filling out their forms- they need ways in which they can actually confirm that humans are the ones making the purchase.

By leading a valiant effort against malicious cyber behavior Nike emphasizes the quintessential idea that online user behavior can never be trusted. According to Positive Technologies report, "Web Application Vulnerabilites in 2017", denial of service (DOS) attacks, the inability to access a web application, are the most common threat for e-commerce, affecting 75 percent of e-commerce web applications.[6] The same bots that are used to buy sneakers can be altered to take down ecommerce applications, which means much more than just an unfair marketplace but rather the inability to make purchases at all. For online retailers, a denial of service attack can mean devastating financial losses. With companies like Nike leading the charge, sneaker companies show that they not only can make significant headway toward developing a fair online retail experience, but also shed significant light into how to maintain awareness toward, and ultimately combat against, much larger bot attacks.

HOW SNEAKERBOTS WORK:

When sneaker retailers first took to the Internet for releases in 2011, browser automation quickly became the preferred method to obtain shoes. Software-testing frameworks like Selenium allowed anyone with basic coding knowledge to automate the process of navigating through a site, adding the shoe to the cart, and filling out the checkout form.[7] It became obvious to retailers that anyone familiar with their online platforms could write a few lines of code and suddenly checkout in a matter of seconds. To combat this scenario sites changed their layouts between releases, so that customers who used pre-automated processes would not be successful. As a result, developers recognized simple browser automation was not reliable enough for the largest releases, and turned to servers to run more complex programs, sneaker-bots, to make sure they would obtain their desired sneakers. [8]

At their core, sneaker-bots automate the check out process; however, they simulate hundreds of customers running through the checkout process, on multiple different sites, in a matter of seconds. Bots bypass the browser and communicate directly with the server to achieve an even faster rate of checkout, and, in the case of the Kanye West's recent Adidas Yeezy releases, "allow users to skip the queue on adidas.com and add the product to cart, which is why many were stuck with a loading screen for hour after hour."[9] An analysis of a popular open-source sneaker-bot shows it uses PhantomJS, a headless browser, meaning a browser that executes processes much faster as it does not use a graphical user interface. Diving deeper into the code reveals that the bot uses proxies as well, to simulate numerous user requests coming from different IP addresses. [10] The headless browser, coupled with numerous IP addresses, gives the customer using this bot a significant advantage over the human clicking through a site, as it simulates numerous customers, moving at a far quicker rate, making attempts to purchase a shoe.[11]

Sneaker-bots are not just limited to personal scripts written by tech-savvy sneaker-heads, but rather there are commercial products, such as AIObot, that utilize more advanced techniques and increased computing power. While AIObot uses proxies, it also makes use of Virtual Private Servers (VPS). A VPS allows a computer to connect remotely to a server, which runs the program. The advantage is that the server has more memory than the user's machine, meaning quicker transaction times, and it is physically closer to the retailer's server, which also decreases the transaction times. Further, AIObot uses Captcha solving services. So, when a person runs a bot which makes numerous attempts to checkout on different sites, if presented with Captchas, the Captchas are uploaded to the service's server and a worker solves the captcha for the person running the program.[12] What makes sneaker-bots so difficult to detect is that they reproduce human behaviors; however, retailers learned to never trust their users and took defensive measures to move toward bot-proof checkout processes.

DEFENSES:

Building a bot-proof website proved to be a nearly impossible task. As security precautions, companies tried to implement Captchas, block IP addresses, and create checkout timeframes that dictated how much time needed to pass before a customer could checkout.[13] However, with overloads of traffic and quick moving customers, these efforts failed because the methods did not differentiate between human and bot activity. Kith, the same boutique that popularized online sneaker releases, worked with Shopify to implement a system in which a trivia question was posed to customers as part of the purchasing process. For websites, this "has proven to be a success in the first line of defense against automation." [14] The idea of implementing features that only real humans can bypass caught on amongst sneaker retailers. To take advantage of this concept, many of the largest names moved away from traditional websites and onto Native apps.

Native apps, applications downloaded through an application store, not only limit exposure to easily manipulated web traffic, but also take advantage of technologies such as biometric authentication and augmented reality to prevent bots from purchasing sneakers.[15] One application that found success in limiting bot use is Copdate, an application that allows stores to set up a reservation system for sneaker releases. Andrew Raisman, the founder of Copdate described how the application works:

> "Our system revolves heavily upon a unique device identifier… it's an actual piece of DNA, or code, that goes into the device. That number is stored in Apple, Google, and all of these databases. Before we let a user access an event that's taking place, we first validate the identifier of the device talking to us is legit. If that device identifier is legit, then we ping it with Apple."[16]

Confirming a user's unique device identifier matches their identity registered with Apple is a way to avoid the dilemma that proxies create, where one user simulates hundreds of attempts to purchase a shoe. With the addition of biometric authentication, like a face or thumb print scan that cannot be replicated by bots, the platform could become even more secure.[17]A platform like Copdate is a great alternative for smaller retailers whose sites are often the most easy to automate.

As the leader in sneakers it comes with no surprise that Nike is also the trailblazer in the fight against bots. Nike migrated all of its limited releases to its app SNKRS, which for its most exclusive releases offers a raffle platform, where users fill out payment information ahead of time and are randomly selected to purchase the shoe, a feature that has not seen any bot activity.[18] Nonetheless, Nike also took measures to make sure every release was not left to random odds. Nike implemented an augmented reality feature called SNKRS Stash Squad- Nike's way of "democratizing the culture". Nike releases stash spots within actual US cities, where users have the opportunity to scan items like posters or statues with their phone to unlock access to sneakers. However, for those who are not located in the city with the stash spots, they can join teams of other users who are in the stash city and if a teammate finds the stash spot then their teammates get to purchase the shoes as well.[19] Digital Trend's Keith Nelson Jr. writes, "By making highly coveted sneakers… available only via an app and scavenger hunt, s23NYC [Nike] essentially rendered bots useless for them." Nike confirmed they have yet to see any bot traffic with the AR features. [20] A key lesson to learn from Nike's endeavors is that an effective way to distinguish bots is to challenge them with processes that require human intuition and interaction.

CONCLUSION:

Sneakers cause a small portion of overall online traffic, but by analyzing how bots affect and influence this traffic significant insights can be drawn as to how to prevent larger malicious bot attacks such as a DOS. DOS attacks are ecommerce applications biggest threat, and bringing together a network of bots is a very effective way of carrying out a DOS. The same precautions sneaker retailers take to distinguish and prevent malicious bot activity are safeguards that too many ecommerce applications ignore. Some of the most important DOS precautions: controlling how many users can communicate with a web server at a time, filtering out malicious IP addresses, and timing out unresponsive connections, are exactly what sneaker retailers had to integrate within their systems.[21] Considering DOS attacks at an even higher level, whenever producing an application that takes on high levels of traffic, it is important that user behavior is constantly questioned rather than trusted. The sneaker industry is a prime example that whenever building a new website or application it is best to think about how it will be abused by hackers. When one builds to withstand attacks, like Copdate or Nike, both the user and producer of the application benefit from a fair, reliable, and secure platform.

[1] Ofiaza, Renz. "Jeff Staple Talks About How the 2005 Nike SB Pigeon Riot Change Sneaker History." *Highsnobiety*. 23 Feb 2018. https://www.highsnobiety.com/p/jeff-staple-nike-sb-

[2] Oliver, Andy. "How Sneaker Retailers are Fighting to Beat the Bots." *Complex.* 28 November 2016. http://www.complex.com/sneakers/2016/11/how-sneaker-retailers-are-fighting-to-destroy-bots

[3] "Global Top 100 Companies by market capitalization". *PWC.* 31 March 2017. https://www.pwc.com/gx/en/audit-services/assets/pdf/global-top-100-companies-2017-final.pdf

[4] Nelson Jr., Keith. "50 year's in, Nike's new digital studio defends its title as king of the kicks." *Digital Trends.* 26 March 2018. https://www.digitaltrends.com/outdoors/inside-s23nyc-the-digital-studio-keeping-nikes-tech-relevant/

[5] Danforth, Chris. "The Bot Problem is Only Getting Worse an Nike Has the Only Answer (So Far)." *Highsnobiety.* 27 April 2016. https://www.highsnobiety.com/2016/04/27/sneaker-bots-how-do-they-work/bots-how-do-they-work/

[6] "Web Application Vulnerabilites in 2017." *Positive Technologies.* 2017. https://www.ptsecurity.com/upload/corporate/ww-en/analytics/PT-AI-Statistics-2018-eng.pdf

[7] Danforth, Chris. "The Bot Problem is Only Getting Worse an Nike Has the Only Answer (So Far)."

[8] Oliver, Andy. "How Sneaker Retailers are Fighting to Beat the Bots."

[9] Danforth, Chris. "How Sneaker Bots Infiltrated adidas YEEZY Boost 350 V2 Release." *Highsnobiety.* 11 October 2016. https://www.highsnobiety.com/2016/10/11/adidas-yeezy-sneaker-bots/

[10] https://github.com/theriley106/SneakerBotTutorials/blob/master/main.py

[11] https://github.com/theriley106/SneakerBotTutorials/blob/master/main.py

[12] "11 Tips for Increasing Your Sneaker Copping Power." *AIObot.* https://www.aiobot.com/11-tips-increasing-sneaker-copping-power/

[13] Danforth, Chris. "The Bot Problem is Only Getting Worse an Nike Has the Only Answer (So Far)."
Schwartzberg, Lauren. "The Botmakers Who Rule the Obsessive World of Streetwear." *Wired.* 25 April 2017. https://www.wired.com/2017/05/using-bots-to-buy-supreme-limited-edition-streetwear/

[14] Oliver, Andy. "How Sneaker Retailers are Fighting to Beat the Bots."

[15] Oliver, Andy. "How Sneaker Retailers are Fighting to Beat the Bots."

[16] https://www.digitaltrends.com/outdoors/sneakers-internet-resale-ebay-feature/

[17] Oliver, Andy. "How Sneaker Retailers are Fighting to Beat the Bots."

[18] Danforth, Chris. "The Bot Problem is Only Getting Worse an Nike Has the Only Answer (So Far)."

[19] Nelson Jr., Keith. "50 year's in, Nike's new digital studio defends its title as king of the kicks."

[20] Nelson Jr., Keith. "50 year's in, Nike's new digital studio defends its title as king of the kicks."

[21] Rubens, Paul. "6 Tips for Fighting DDoS Attacks." 25 January 2016. *eSecurity Planet.* https://www.esecurityplanet.com/network-security/5-tips-for-fighting-ddos-attacks.html