BOTS

In technology and digital marketing circles, there is often talk of "bots". Some people say they are necessary so that search engines can "discover" content. Other times bots can cause harm to websites, servers, and users' computers. Recently, bots have been called out as a major problem for online advertising, with a recent Wall Street Journal article citing that 33% of online advertising traffic is from bots. Perhaps you've even heard the term "Malvertising" (malware + advertising) that is used to describe this problem.

Whether they are good, bad, or benign, the question still remains, "What is a bot, exactly? It's like the Boogeyman – I've heard of it, people talk about, but I've never seen it."

WHAT'S INSIDE

The goal of this document is to help shed light on what has become the "boogeyman" of Internet advertising by answering the following:

- What are bots?
- What do bots do?
- Should I be worried about bots from LotLinx or its Affiliates?
- Does Google Analytics weed out bot traffic?
- How does LotLinx weed out bot traffic so I pay for Shoppers, not robots?
- What do I do if I think I detect bot activity in my reporting?

Presented by befoundonline the art and science of digital marketing

WHAT ARE "BOTS"?

An Internet bot, also known as web robot, WWW robot or simply bot, is a software program that runs automated tasks on the Internet. Typically, these are tasks that are too repetitive and numerous for a human user to do in a reasonable amount of time. The nature of bots can run the spectrum from benign (even positive) to extraordinarily harmful.

When search engines such as Google and Bing crawl your site looking for new, relevant content, this is being done by a bot. It's simply crawling all of the content and meta data on your site, so it can serve these pages in search queries later. This is good. In most cases, you want search engine bots crawling your site, to ensure that your newly created content is being quickly indexed.

On the opposite end of the spectrum, there are also malicious bots. These are the ones that most likely come to mind when we think of bots. There are 'spambots' that crawl comment, review, contact, or guestbook pages and harvest email addresses to eventually spam. There are malicious bots designed to take down websites. There are also bots created to drive "clicks" off of advertising, so that a web publisher can drive up site revenue.

WHAT WOULD "BOTS" DO ON A WEBSITE?

Large, frequently updated sites (like many LotLinx Affiliate sites) are regularly visited by all types of bots. As mentioned earlier, though, not all bot traffic is necessarily bad news.

Some of the bot traffic is undoubtedly coming from search engines that website owners want to have visit their site on a frequent basis. This will help ensure the latest version of your site is being indexed in search engines, such as Google, Bing, and Yahoo.

On the other hand, some of this bot traffic could be from page scraping bots. These are bots that crawl through pages and copy its content to use on other pages. With the sheer amount of valuable automotive content on LotLinx partner websites (such as reviews, specifications, and VIN numbers), there is the likelihood that these bots could be scraping this for use on other pages or for data analysis.

Additionally, there are bots that do false form submissions. These are bots that detect lead generation forms – such as those on a VDP page – and submit fake information. Much like the page scraping bots, false form submission bots are relatively commonplace on sites that have lead generation forms. While they are a nuisance and send useless leads, they do not pose a virus threat to users of the site.

Bots that have received a significant amount of attention recently are bots that "click" on web ads. These bots can be deployed by greedy publishers looking to grow their ad revenues, or even by bots that are designed to follow any links on a site. Finally, there are bots that could potentially harm web users. One way these malicious bots could manifest is as viruses or worms that would be installed on a user's computer. If a particular site was infected with malicious bots, user's computers would be infected with a virus once they took a certain action, such as clicking a link or downloading a file.

SHOULD I BE WORRIED ABOUT "BOTS" FROM LOTLINX OR ITS AFFILIATES?

The three types of bots that are likely visiting LotLinx partner websites are essentially benign, in terms of visitor safety/viruses. The first type of bot is a search engine bot, crawling the site(s) for content to index in its search results. The second type of bot is a content scraper, which is a relatively common practice on the Internet today and doesn't normally pose any security/virus threats to site users. The third type of bot is a false form submission bot and, again, while it's a nuisance to site owners, is essentially benign.

Even more, LotLinx works with high caliber sites looking to help car Shoppers ind their next set of wheels – not grow revenue in unethical manners.

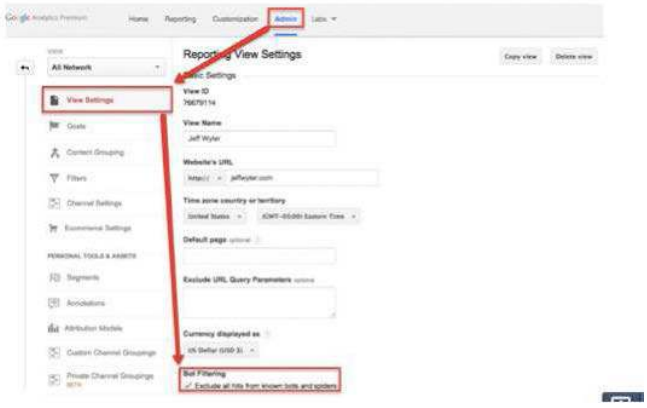
Plus, LotLinx deploys sophisticated bot detection techniques to protect dealer customers from harmful bots and Lotlinx Bots Whitepaper - Presented by Be Found Online 2 from paying for traffic from robots. Specific ways LotLinx battles bot traffic are detailed at the end of this document.

While there is always the risk with any site that more malicious bots may be present, most websites deploy software designed to detect and eliminate these bad bots.

DOES GOOGLE ANALYTICS WEED OUT "BOT" TRAFFIC?

Yes. As of late July 2014, Google released functionality that allows Google Analytics users to easily filter out traffic to their site that comes from known bots. This functionality looks out for – and filters out – bots on the IAB "International Spiders & Bots List". The IAB (International Advertising Bureau), with the guidance of bot experts from companies such as Google and AdTech, maintains a frequently updated list of known bots.

When traffic from one of these bots hits one of your pages, Google filters it out, only delivering the real number of visitors that are coming to your site. A best practice is to also enable Bot Filtering in Google Analytics – and is something we highly recommend. Here is where you can "check the bot filter" box in the Admin tools within GA:



That said, it is an ongoing process of identifying and filtering bot traffic, as new ones are constantly being created and deployed across the web.

HOW DOES LOTLINX WEED OUT "BOT" TRAFFIC SO I PAY FOR SHOPPERS, NOT ROBOTS?

Because LotLinx dealer customers pay to have their VDPs Deeplinked on a CPUS (Cost per Unique Shopper) basis, being experts in Bot detection is core to our business. We dedicate significant resources to bot detection, in order to ensure that our dealer customers invest their ad dollars in driving Unique Shoppers, not robots, to their VDPs. LotLinx' efforts to weed out bot traffic include proactively filtering known bot traffic as well as reactively scanning and monitoring traffic to ensure new bots are identified and filtered.

LotLinx Proactive Bot Detection:

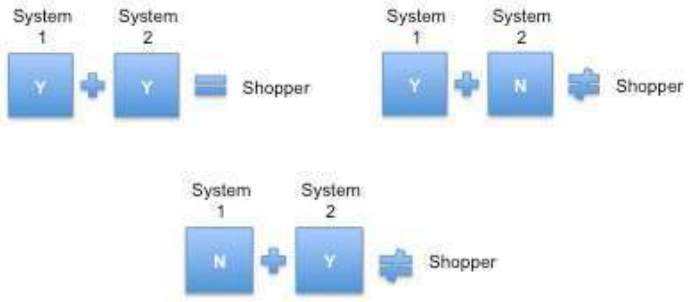
First and foremost, LotLinx works with quality publishers who are passionate about automotive and digital. Each publisher is directly contracted by LotLinx, and commits to never deploy deceptive practices to drive fake traffic across the LotLinx platform. Second, LotLinx Bot detection processes run on daily, weekly and monthly intervals to review traffic for patterns that indicate programmatic page views, versus a live shopper.

Here is a brief description of those programs and processes:

- **JavaScript Redirection:** A large number of bots on the Internet do not and cannot execute JavaScript. They simply connect to a website to parse the returned HTML content. LotLinx's redirection service that sends shoppers to your website is implemented through client side JavaScript code. It was purposefully designed this way to ensures that the majority of crawlers that hit our site, never make it to the dealer site, and are promptly invalidated.

· **Bad Bot List:** LotLinx has developed what we call the "Bad Bot List," which is a compilation of bots we've discovered over the past 2 years and logged in our database. We continuously add to this list as we detect programmatic, not human interaction, patterns in site traffic. Thus, we are able to use our Bad Bot List to identify bots we know to exist on the fly.

· **Shopper Double Verification:** LotLinx deploys two autonomous traffic verification systems to verify that a Shopper is a human, not a bot. If either system believes the traffic is from a bot, we do not charge our dealer customers for that traffic. Here is a simplistic illustration of how Shopper Double Verification works:



· **Third Party Data Sources:** LotLinx also leverages industry services that serve as repositories of bot lists and offer resources for bot detection. For example, we subscribe to Project Honey Pot, an open source initiative that tracks abuse, fraud, and other malicious behavior that occurs online. Similarly, as members of the IAB, we subscribe to the IAB/ABC International Spiders and Bots List.

REACTIVE BOT DETECTION:

As new bots are programmed and deployed daily, we will use our own technology and algorithms to identify them in advance of making the published 'lists' of known bad bots. When new suspicious activity is detected, like emergence of a new IP that is exhibiting activity out of the "norm" for our Shoppers, the identifying information from this traffic is added to our internal data, and used for all subsequent traffic.

On a nightly basis, suspect traffic is invalidated and removed from dealer shopper counts. In the event a pattern isn't sufficient enough to be detected with a single days' worth of data, LotLinx then evaluates the same data over a 7 day period, and again each month, looking back each time to identify any bot traffic that might not have been previously detected. Lotlinx regularly evaluates new services and methods to identify bot traffic, and strives to ensure that only legitimate shopper traffic is charged to the dealer. This is not a simple task, but critical to both LotLinx' success and the success of the dealers receiving the shopper traffic.

WHAT DO I DO IF I THINK I DETECT BOT ACTIVITY IN MY REPORTING?

Short answer is, you will never be charged by LotLinx for non-human traffic. If you discover any suspicious activity, we will refund your money. Period. No questions asked.

If you do see activity that you question, immediately call your LotLinx account manager, or our main line at 800.625.LINX (5469).

By way of example, we recently had one dealer inquire about a large number of visits to one of his VINs (it's rare, but it happens). After analysis, we were able to identify a new (harmless) bot that was being produced from a visit from a very popular social network. None of our nerdy tech friends had even seen this bot before so we were quite grateful for this find.

And, should you find a bot that LotLinx, the IAB and Honeypot haven't already detected, we'll give you 6 months of FREE LOTLINX as a thank you! While finding an undetected bot is extremely rare, we hope you take our challenge seriously and join us in the effort to proactively protect the Internet.

To have your Google Analytics account audited by one of our digital consultants, call 800-625-5469 today or visit lotlinx.com/bots

befoundonline
the art and science of digital marketing

3304 N. Lincoln Ave Chicago, IL 60657
1-877-55-FOUND BeFoundOnline.com

LOTLINX®

412 S. Wells St. Ste. 600 Chicago, IL 60607
1-800-625-LINX LotLinx.com