Understanding Impact of Bad Bots and Pre-Emptive Anti-Bot Protection

All the industries are struggling with one major problem that is bad bot activities that leads to many complex attacks on networks and infrastructure.

NOIDA, UTTAR PRADESH, INDIA, March 17, 2022 /EINPresswire.com/ -- Every industry that utilizes the internet to keep its business up and running has one common issue – The Big Bad Bot Problem. So, what is this problem? It's the bad bots that crawl all over one's web application to gather the information that can further be used by the attackers to exploit the web application. And the solution is bringing anti-bot protection techniques to block and mitigate the bad bot activity.

According to the research done by the R&D department of Haltdos.com, it was found that bad bot traffic has increased 19.2% YoY for the APAC region from 2020 to 2021 whereas for the global region the increase has been stunted to 3.8% YoY from 2020 to 2021. As the increase of bad bot activity for the PAC region has bought much concern in the cyber-security sector, the good bot activity which is important for businesses in terms of ranking on the SERP page has not seen as much growth.

So what are bad bots? They are software applications that run automated tasks over the internet. And when they start reconnaissance activity for potential attackers and start mutating into many advanced bots. Primarily they pretend to be search engine crawlers, easily hiding behind known anonymous proxies and keep on changing IP addresses.

Based on their activity bad bots can now be categorized into four categories. Starting with the very simpler bots, whose sole purpose is reconnaissance and testing exploits. After that, they evolve into headless bots, which usually takes the form of a script that is either run on a scheduled basis or triggered by an event from the external system. The primary objectives of a headless bot can be defined as credential stuffing, scraping and spamming. Then comes a much more sophisticated bad bot category that is capable of mimicking real human behaviour. Under sophisticated bad bots we have interactive bots and behaviour bots that are capable of API abuse, account takeover, carding, scraping, spamming.

According to the research done by the haltdos.com department, traffic distribution of various evolved bot categories are as follows: Simpler bots take the least traffic distribution with just 10%, whereas the majority of the traffic distribution was seen by headless bots with around 45%, as they are majorly deployed in activities like reconnaissance & scraping. Sophisticated bots like interactive bots and behaviour bots have traffic distribution of 30% and 15% respectively.

If we look at the bot activity distribution by industry, we find bad bots wreaking havoc in the financial industry followed up closely by the education and SaaS industry. The lease hit industry by the bad bot activity is Ecommerce and Healthcare industries, closely followed up by gaming and digital content and advertisement industry. Good bot activity majorly plays role in the digital content and advertisement industry whereas there is nearly nil activity of good bots in the gaming industry, according to the research done by the R&D department of haltdos.com, also if we look at the bot activity on specific pages, we find bad bots majorly on the login and product pages, whereas good bots can be seen crawling over homepage, category and product pages.

With simpler anti-bot protection techniques that can be implemented to detect and mitigate bad bots, the most common industry-trusted technique is to implement captcha and JS challenge, which can be thrown at the user who is trying to log in, fill out a form or even at the very first visit on the web application. Having a good anti-bot threat Intel with known malicious user agent dataset, anonymous proxy list and IP reputation for strengthening the anti-bot protection. Further, industry experts believe that verifying the search engine crawler with reverse DNS lookup can help in identifying if the request is coming from a genuine human user or a bot agent. Anti-bot protection can also be further enhanced by continuously monitoring the user session and blocking unsolicited POST requests. But there are also some hiccups when it comes to simpler anti-bot protection techniques such as blocking IPs, Geo-Fencing and blocking bad user agents.

Overcoming the challenges that are faced by simpler anti-bot protection techniques can be addressed by advanced anti-bot protection techniques that industry experts can implement in their solution to bring a much stricter anti-bot protection. Having advanced fingerprinting techniques with advanced detection of human vs automated traffic. HTML elements with dynamic names and ids, browser fingerprinting and TLS fingerprinting are among some advanced anti-bot protection techniques. Further, Client interaction fingerprinting and server-side user behaviour analysis can help in identifying and analysing the activity on the web applications. Implementing mobile SDK and 3rd Party SDK for API to bring in additional anti-bot protection for mobile devices and mobile applications.

Pre-emptive anti-bot protection can be achieved by simply tricking bad bots into a tar pit or furnishing wrongful information via decoys to disrupt the evolutionary chain of bad bots that lets them churn data and helps them to evolve from simpler bots to headless bots and finally too much sophisticated bad bots like interactive bots and behaviour bots. Hence, the pre-emptive defence can be strategized in a three-phase manner. Firstly, Deploy, embed decoy links and forms, create decoy pages and advertise as something you are not. This deployment will act as

the initial sugar-coated candy for bad bots (flies), they will think of it as a genuine source of information and would just pounce on it. Secondly, Monitor, where one has to detect the activity of bad bots on the deployed decoy forms, links and pages. Engaging with the bad bots and learning their behaviour will help the security professional in understanding the bot's intentions. And finally, Block, where you dynamically blacklist bad bot sources, improves bot assessment and creates app-specific bot behaviour.

Anshul Saxena
Haltdos
+91 1800 120 2394
info@haltdos.com
Visit us on social media:
Facebook
Twitter
LinkedIn
Other
