


Crookies: Tampering With Cookies to Defraud E-Marketing

Bede Ravindra Amarasekara

 <https://orcid.org/0000-0003-1744-716X>

Massey University, New Zealand

Anuradha Mathrani

 <https://orcid.org/0000-0002-9124-2536>

Massey University, New Zealand

Chris Scogings

Massey University, New Zealand

INTRODUCTION

E-marketers are on the constant lookout for ways to generate visitor traffic to their e-commerce sites in a cost-effective manner. Search Engine Optimised (SEO) page rankings, paid-search, keyword bidding, *cost-per-mille* display advertising (CPM) and *cost-per-click* banner advertising (CPC) are some of the different ways to attract user traffic; for a fee. With the advent of *Affiliate Marketing* (AM) businesses around the globe found a new way to generate visitor traffic at a relatively low cost, using a network of affiliates (Brear & Barnes, 2008; Norouzi, 2017). Nevertheless, increasing criminal activities on Internet has made CPM and CPC advertising models prone to large scale fraud activities, such as *click-fraud* (Edelman, 2015). In this backdrop, cost-per-acquisition (CPA) appeared as the silver bullet against AM fraud, as under CPA e-commerce sites do not pay for *clicks* or for page visits anymore. The affiliates are instead rewarded only for monetary outcomes (Hu, Shin, & Tang, 2013). Though CPA is considered the safest and most cost-efficient visitor traffic generation model for Small-to-Medium Enterprises (SME), the discovery of *cookie stuffing* fraud shows that it is not the silver bullet that it was thought to be. Though at a much lesser degree, some fraudulent activities have been recently discovered (Amarasekara, 2017; Chachra, Savage, & Voelker, 2015; Edelman & Brandi, 2015).

During this research an AM strategy of a current practitioner was examined. Two datasets of AM-generated web traffic data were analysed to detect any possible fraudulent patterns. These two datasets were separately generated by two different Affiliate Marketing Networks (AMN) that managed AM services for the same practitioner at two different periods of time. A test environment was developed, named AMNSTE (Amarasekara & Mathrani, 2016), which can simulate the complete set of processes that underlie web-traffic generation within a real-world AM network, using the same underlying technologies. AMNSTE consists of multiple virtual servers within different web domains. They are connected by virtual switches and routers that allow inter-domain routing. While AMNSTE has the ability to add new domains and additional servers, a minimum test configuration comprises of three web domains, each representing one of the three stakeholders in AM: Advertiser (e-commerce site), the AMN (tracking service provider), and at least one Affiliate website. Each of the three domains comprises a web server to host the website or web-services and a database server to save transaction and tracking data. Fraudulent

DOI: 10.4018/978-1-5225-9715-5.ch073

actions discovered within datasets were tested through simulations on AMNSTE, and multiple fraudulent methods were discovered to execute some of the currently known frauds. AMNSTE also allowed the authors to discover newer vulnerabilities that can be used by fraudsters in future, to defraud AM networks. The solutions proposed here were tested on AMNSTE for efficacy and utility.

This paper provides an insight in to how cybercrime is effecting e-commerce activities by endangering one of the most affordable and cost-effective traffic generation models available to SMEs. The paper first introduces the reader to the topic of Affiliate Marketing, and the underlying tracking technology based on the HTTP cookie. Then, it provides a technical perspective to the frauds that are currently known such as *Cookie stuffing* by explaining how those frauds are accomplished. It then describes new vulnerabilities that have been discovered by the authors during their current research project, which could be exploited by fraudsters in future. Next, the authors propose solutions on how to mitigate the risks, which would enable e-commerce practitioners to implement new solutions or re-examine their existing security strategies. Finally, the conclusions and future research directions are discussed that could make the tracking system more robust and reliable, in order to sustain this cost-efficient and affordable marketing model.

BACKGROUND

Affiliates are independent websites who already have a large following of visitor traffic, who might belong to the potential target market of some product advertisers. Affiliate marketing model uses a network of such affiliates, who will promote the advertiser's website, usually by displaying a banner advertisement. Figure 1 provides a logical view of the AM process, starting from a visitor's click on a banner advertisement at an affiliate's website to the completion of a purchase action. The sequence of the processes involved are numbered in the diagram. When a user views an affiliate website (process 1) and clicks an advertisement link (process 2) the "Click Pixel" embedded in the webpage causes the tracking server to create a record of the "click" action in the database (process 3). The tracking server then sends a cookie to the browser with a unique identifier that refers to this specific click. It also sends a redirect response to the browser, targeted at the advertiser's e-commerce site (process 4). The visitor then browses the e-commerce site and makes a purchase decision (process 5). The process 6 is abbreviated as "AN Res. Rq.", which stands for "Affiliate Marketing Network resource request", which refers to the "Conversion Pixel" embedded in the payment confirmation page sent by the e-commerce serve. In the background without any visible clue to the user the *Conversion Pixel* causes the user's browser to send a resource request to the tracking server with the information such as the Invoice Identifier, total purchase price, etc. as parameters of the resource request. As every HTTP request to the web server is accompanied by the cookies that the server has set previously, in this case during the click-tracking process numbered 3, the tracking server records the sales conversion details against the click-tracking data in the database. The *Click Pixel* and *Conversion Pixel* are small pieces of JavaScript code that are embedded in those webpages that provide user-specific information to the tracking server. The tracking server, while being invisible to the user, keeps track of all processes and traffic movements with the help of *tracking-cookies*. Next, how the above cross-domain tracking systems are used by different marketing models are discussed.

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/crookies/248105

Related Content

Innovation and Corruption in Turkey: "Grease the Wheels" or "Sand the Wheels"

Hülya Ünlüand Merve Karacaer Ulusoy (2021). *Handbook of Research on Theory and Practice of Financial Crimes* (pp. 80-103).

www.irma-international.org/chapter/innovation-and-corruption-in-turkey/275453

A Comparative Analysis of Laws Amongst Western Powers Through the 20th Century

(2023). *Comparing Black Deaths in Custody, Police Brutality, and Social Justice Solutions* (pp. 30-66).

www.irma-international.org/chapter/a-comparative-analysis-of-laws-amongst-western-powers-through-the-20th-century/323584

Interventions for Sexual Abuse

Prathibha Augustus Kurishinkal (2018). *Social, Psychological, and Forensic Perspectives on Sexual Abuse* (pp. 259-283).

www.irma-international.org/chapter/interventions-for-sexual-abuse/197832

The Evolution of Active Shooter Protocols on College Campuses

Tanya M. Grantand Makayla S. Dole (2020). *Handbook of Research on Mass Shootings and Multiple Victim Violence* (pp. 289-306).

www.irma-international.org/chapter/the-evolution-of-active-shooter-protocols-on-college-campuses/238581

Regulatory Ambiguity: The Underbelly of Insider Trading

Laura Pinto Hansen (2021). *Handbook of Research on Theory and Practice of Financial Crimes* (pp. 132-148).

www.irma-international.org/chapter/regulatory-ambiguity/275456