Exploiting Online Targeted Advertising

Wei Meng, Xinyu Xing, Anmol Sheth, Udi Weinsberg, Wenke Lee
Georgia Institute of Technology, Technicolor

Online targeted advertising is one of the primary approaches used to monetize the “free” online services and applications available to users. Recently, there has been a concerted effort made to increase the relevancy of ads targeted at users. Studies have shown that ads targeted based on the user's online interests have a 40% higher chance in leading to a financial conversion over non-targeted ads [1]. Consequently, the average price online advertisers and marketers are paying for these target ads is 2.6× higher than non-targeted ads.

The revenue model for online targeted advertising can be approximated by the function of three primary entities: *ad exchange platforms, advertisers, and publishers*. Ad exchange platforms (e.g., DoubleClick) facilitate connections between the advertiser (e.g., Toyota) and publisher (e.g., www.kbb.com) by providing a real-time bidding platform for buying and selling ads. Publishers register their website with the ad exchange and host ad slots. Advertisers set up their campaign by describing the user demographic and interests they wish to target, along with a maximum cost they are willing to pay for ad impressions or clicks delivered to their target audience. The ad exchange runs an online auction based on the bid values from all the competing advertisers and delivers the winning ad to the user visiting the publisher page. The revenue generated from this transaction is shared between the publisher, which typically receives 68% [2] of the revenue, and the ad exchange platform. As is evident from this description, there are two main factors that impact the publisher's revenue: (1) the number of users visiting the publisher webpage which in turn impacts the number of ad impressions or clicks served by the publisher, and (2) the cost that advertiser are willing to pay to have their ads targeted at users visiting the publisher page.

Existing approaches available to publishers to increase their ad revenue primarily rely on increasing the traffic volume to the publisher page and consequently the number of ad impressions or clicks. Examples of legitimate approaches include advertising the website on search engines or other related websites to drive more traffic to the publisher's website from search results. Alternatively, a publisher can increase the page rank in search results using a range of Search Engine Optimization (SEO) technique, such as, hosting relevant and frequently updated content. However, these approaches are not straightforward and quite expensive to scale. Alternatively, fraudulent approaches rely on driving “fake'” traffic to the publisher website by participating in pay-per-view networks [3] that increase the number of ad impressions or subscribing to botnets that generate fake clicks on ads hosted by the publisher website [4].

In this talk, we present a novel fraudulent method for publishers to increase their ad revenue from visitors to their websites. Our method can be either used as a stand-alone method, thereby increasing revenue from real, legitimate users, or alternatively in conjunction with exiting methods thus increasing the revenue from both real and fake visitors. Our mechanism enables publishers to increase their ad revenue by misleading advertisers and ad exchange platform to deliver higher paying targeted ads to the visitors of the compromised publisher page. Our attack exploits the fact that advertisers set up ad campaigns to target audiences with specific online interests and the interest profile can be polluted by vulnerabilities like cross-site scripting that is not detectable by the ad exchange platform. To launch such an attack, the publisher hosts custom JavaScript code that loads webpages in a camouflaged manner from specific interest categories. These “fake” visits in turn pollute the user's online advertising profile such that when the user returns to the publisher page she is more likely to be targeted ads related to the polluted profile. While complementary to existing ad fraud mechanisms, this attack can be used in conjunction with existing attacks to further increase the ad revenue.

We address a number of challenges involved in making the above described attack practical and effective for the existing ad targeting ecosystem. First, we seek to develop a practical approach to pollute the user's ad profile that works across the two commonly used ad targeting mechanisms of behavioral targeting and re-marketing. Second, the profile pollution should be effective in drawing higher paying ads to the publisher page across a wide range of pre-existing user profiles. Third, the attacker should be able to estimate the expected revenue increase given the frequency of revisits of users to the publisher page.

Reference

[1] Ayman Faraha, Michael C. Bailey, “How Effective is Targeted Advertising?”, Proceedings of the 21st international conference on World Wide Web, 2013.
[2] https://support.google.com/adsense/answer/180195?hl=en.
[3] Kevin Springborn, Paul Barford, "Impression Fraud in On-line Advertising via Pay-Per-View Networks", Proceedings of the 22nd USENIX Security Symposium, 2013.
[4] Vacha Dave, Saikat Guha, and Yin Zhang, "Measuring and Fingerprinting Click-Spam in Ad Networks", Proceedings of the Special Interest Group on Data Communication. 2012.