Armored Ads

Wesley Brandi
iPensatori
Seattle USA
wbrandi@ipensatori.com

Brendan Kitts
Applied AI Systems
Seattle USA
bkitts@appliedaisystems.com

Raj Mahato, Jing Ying Zhang
Microsoft
Seattle USA
rmahato@microsoft.com

***Abstract*—Ad Servers monetize by sending ads to a requesting publisher which renders them on their web page. The Publisher receives a commission if the ad is clicked. Unfortunately, fraudulent publishers may try to request ads and click on them through a variety of fraudulent schemes including robotic traffic, deceptive placement, and distribution across other sites. Armored ads are designed to thwart these attempts and are also designed to serve as a probe into whether traffic is human or robotic.**

***Keywords*—bot; click fraud; PPC; sponsored search.**

I. Introduction

Click Fraud scams come in many varieties. One technique used by fraudsters is to request ads from an Ad Server, copy out the links, and then click on them fraudulently. A fraudulent publisher can request, cache, and then deploy hundreds of ad links across a variety of sites and in a variety of locations that were never intended by the ad-server, in order to generate revenue for their website.

In this paper we propose a method for increasing the security of ad links that we call "Armored Ads" which has been described previously in concept (Kitts, et. al., 2007).

An Armored Ad is an ad that is rendered in an executable and has an obfuscated link structure. The link that appears in the ad box is actually a button. These ads can only be clicked by manually navigating the mouse over the ad link. After clicking on an Armored ad, the location of the click is passed to the Ad Server for analysis.

This serves two useful purposes: Statistics can be developed on a publisher's performance in terms of handling Armored Ads. If the publisher almost never successfully clicks on Armored ads, but clicks on everything else, then it would suggest that the Publisher is using automated systems to create fake clicks.

Secondly, the Armored ad also protects the link contents, and ensures that they can't be re-deployed to different sites.

References

[1] Daswani, N. and Stoppelman, M. (2007) The Anatomy of ClickBot A, Usenix, HotBots 2007, http://static.usenix.org/event/hotbots07/tech/full_papers/daswani/daswani.pdf

[2] Daswani, N., Mysen, C., Rao, V., Weis, S., Gharachorloo, K. and Ghosemajumder, S. (2008) Online Advertising Fraud, in Jakobsson, M. and Ramzan, Z. (eds), Crimeware, Symantec Press http://shumans.com/onlineadvertisingfraud.pdf

[3] Edelman, B. (2006) The Spyware - Click-Fraud Connection -- and Yahoo's Role Revisited, April 4, 2006, http://www.benedelman.org/news/040406-1.html#e1

[4] Kitts, B. (2006), Click Fraud Protector, US Patent Publication Number US 2008/0114624 A1

[5] Kitts, B., Najm, T., Burdick, B. (2007), Identifying Automated Click Fraud Programs, US Patent Publication Number US 2008/0281606 A1

[6] Kitts, B., Zhang, J., Wu, G., Brandi, W., Beasley, J., Morrill, K., Ettedgui1, J., Siddhartha, S., Yuan, H., Gao, F., Azo, P., Mahato, R. (2013), Click Fraud Detection: Adversarial Pattern Recognition over 5 Years at Microsoft, unpublished.