

AIT Exposes New Click Fraud Technique

Date: 04-19-2007 08:25 PM CET

Category: [IT, New Media & Software](#)

Press release from: [Advanced Internet Technologies, Inc.](#)

(Fayetteville, NC) Web Hosting Company (AIT) AIT.com home to over 210,000 websites accused the Fayetteville Observer, fayobserver.com or the Fayetteville Publishing Company (FPC), of committing online Click Fraud against its local and national advertisers. The paper, AIT alleges, is part of an ever growing syndication of click affiliated sites receiving revenue generated from Click Fraud. "We have seen all kinds of techniques for committing Click Fraud," said Clarence Briggs, AIT CEO and former U.S. Army Infantry Officer. "We have seen software programs that automate the process of Click Fraud. Then there is the manual fraud where people click on online ads over and over with no intent of buying anything but just to get paid a percentage of each click – pay to surf and click. Lately, we have seen click BOT armies doing it." AIT is the company that charged Google with click fraud and led the class action lawsuit against the search engine last year. AIT also worked with the FBI on the matter and started the Click Fraud portal www.igeryon.com. "Ironically, Google and other search engines might be the victim in this instance," said Briggs.

Briggs has labeled the most recent Click Fraud as the "Bang Box" scheme. "It is ingenious," said Briggs. He describes a situation where a publisher like a local newspaper hosts its web servers in a data center with an ISP. The newspaper or publisher then gets fed advertiser ads from the search engines, syndicates and other IAB members to its web site. Then they hire a third party to rent a web server inside the ISP's data center in order to click on the ads without generating suspicious external traffic. They are paid for the clicks by the search engines. AIT like many other local and national advertisers had placed a significant amount of online advertising on the Fayetteville Observer's web site. AIT is also the technology company which provided co-location for the Observer's web servers in the AIT data center. When AIT grew suspicious that it was being over-billed for advertising, AIT as a web-host was able to monitor web traffic to and from the Observer's web site asserted Michael Roberts, the CIO of AIT. According to Roberts, "AIT determined that up to 50% or more of the online impressions and ad clicks for which the Observer charges AIT and other advertisers were artificially manufactured or inflated. Roberts claimed AIT was able to gauge traffic to and from the newspaper's website which far below the statistics the Observer used to attract advertisers in its online policies and agreements. Charles Broadwell, the Publisher of FPC, could not be reached for comment

"The FPC rate card and other representations made by the Observer claimed they got 17,000 visitors a day to their website", said Briggs, "This is simply not true. We recorded and documented a few genuine visits a day, but the majority of visits were manufactured by the Bang Box. We wanted to open and examine the Observer's web servers in front of everyone and the court to get at the truth and prove the fraud but they did not want to do so." Briggs says that AIT has compiled a list of both national and local advertisers who could be victims of the FPC click fraud. He indicates that they will contact the possible victims to let them know that they have hard evidence of the wrongdoing committed against them. Briggs also says he will contact the search engine syndicates and send them the evidence he has regarding FPC. "It just may be possible that this sort of thing is widespread - publishers inflating traffic without the search engines knowing about it." Briggs will be the keynote speaker at ISPCON this year www.ispcon.com/conference/keynotes.php. ISPCON is the capstone event for the Internet industry and Briggs says he intends to use the FPC experience to expose the anatomy of click fraud from the search engines and syndicates down to local publishers. "We are going to put the entire lawsuit and discovery online," said Briggs. "Folks have a right to know the truth."

Recently, AIT certified its network as "clean" of crimeware and malware with Panda Software's Malware Radar. Panda Software www.pandasoftware.com discovered the malicious "Clickbot.A" and is a pioneer in the industry combating malware, Trojans and viruses. "Many ISPs inadvertently allow malware to be used by their networks to commit illegal or unethical acts", says Ryan Sherstobitoff, Product Technology Officer for Panda in the U.S. "Malware Radar is a product we developed to assist ISPs to combat the problems and prevent their network resources from being abused." AIT and Panda have partnered and are working with the FBI to identify and stop Malware. We intend to use all the data and evidence from surrounding this Bang Box scam to educate the public about click fraud. We actually have film footage in real time that we can release showing the generation of false traffic." Briggs says that based on the circumstances of this Click Fraud scheme, no

one has ever had this level of evidence. For more details visit www.igeryon.com.

A Staff Report

web hosting
complex hosting
web design/development
VoIP solutions
Ecommerce
Security/Monitoring

Advanced Internet Technologies, inc
421 Maiden lane
Fayetteville, nc 28305
910-321-1200

[You can find this press release here](#)