

Cookie Stuffing Studie

2011

(Öffentliche Version)

Affiliate Marketing Studie

Im Vorfeld der Studie haben wir uns Gedanken gemacht wie Betrug im Affiliate Marketing funktionieren könnte und im Anschluss dazu einige Testläufe durchgeführt.

Die Ergebnisse waren teilweise so schockierend, dass wir sie an dieser Stelle nicht vollständig veröffentlichen können. Dieses gilt besonders für die Skripte und Tools, die einfach nachgebaut werden können. Bitte haben Sie Verständnis, dass wir nicht noch mehr Affiliates in Versuchung führen wollen schnell Geld zu verdienen und daher auf eine Veröffentlichung verzichten.

Das Hauptaugenmerk unseres Tests lag darauf, wie die Anmeldung zu einem Affiliate Programm umgangen werden kann. Ohne Angabe persönlicher Daten haben wir verschiedene Partnerprogramme getestet und auf Anhieb bei **über 600 Partnerprogrammen** einen Trackingcode, der unsere Sales registriert hat binnen 3 Min. erhalten.

Mit dem so erhaltenen Trackingcode waren **Cookie Stuffing /Dropping** im kleineren Ausmaß, Brand-Bidding, sowie weitere illegale Transaktionen einfach zu realisieren. Die Account Manager und Agenturen haben den Betrug nicht bemerkt und die Provisionen wurden uns im Netzwerk gutgeschrieben. Selbstverständlich haben wir nach unseren Tests den Account bei allen Partnerprogrammen gekündigt und die Provisionen nicht erhalten.

Cookie Stuffing vs. PostView

Zunächst möchte ich den Unterschied zwischen Cookie Stuffing und PostView aufzeigen. Wir haben für unsere Tests Cookie Stuffing betrieben, also ein nicht vom Merchant freigegebene Methode, mit der wir über verschiedene Techniken Cookies bei Ihren Kunden platziert haben.

Die Werbemittel aus den Affiliate Netzwerken wurden hierbei zwar sichtbar wie beim PostView angezeigt, wir hätten diese aber auch nicht anzeigen müssen.

Der Schaden liegt bei Ihnen als Merchant, da Sie beim Cookie Stuffing keine Werbeleistung erhalten. Weiterhin werden die „guten“ Affiliates geschädigt, deren Cookies von den schwarzen Schafen überschrieben werden.

Beschreibung	Stuffing	PostView
<i>Erlaubnis vom Merchant</i>	<i>Nein</i>	<i>Ja</i>
<i>Anzeigen der Werbemittel</i>	<i>Nein</i>	<i>Ja (min. 120x60)</i>
<i>Schaden beim Merchant</i>	<i>Ja</i>	<i>Teilweise</i>

Stuffing Methoden

Es gibt derzeit drei unterschiedliche Cookie-Stuffing Methoden, mit denen es Affiliates möglich ist ein Cookie bei einem Kunden zu platzieren. Die Cookies werden hierbei unbemerkt vom Affililiate durch ein Iframe im Quellcode, einen Browser, oder eine Flash Datei gesetzt.

Iframe: Im Quelltext einer Internetseite kann ein Iframe aufgerufen werden, das über einen Trackinglink Ihre Seite aufruft. Dieses wird meistens für eine Vorschau einer Seite verwendet. Setzt man aber die Länge und Breite auf 1px so sieht der Kunde das Iframe nicht und der betrügerische Affiliate kann beliebig viele öffnen.

Firefox: Der Firefox hat einen sehr großen Marktanteil im Browsermarkt eingenommen. Affiliates ist es mit „Firefox Prefechting“ ebenfalls möglich Cookies unbemerkt beim Kunden zu setzen. Der Browser Firefox „prefetcht“ die Inhalte solcher Seiten, von denen er davon ausgeht, dass der Nutzer sie bald sehen will. Interessant ist dabei, dass man Firefox durch ein einfaches Tag dazu bringen kann, Inhalte und Cookies zu „prefetchen“.

Ein Beispiel haben wir hier auf der Seite bereitgestellt: <http://www.fsom.de/prefetch.html>

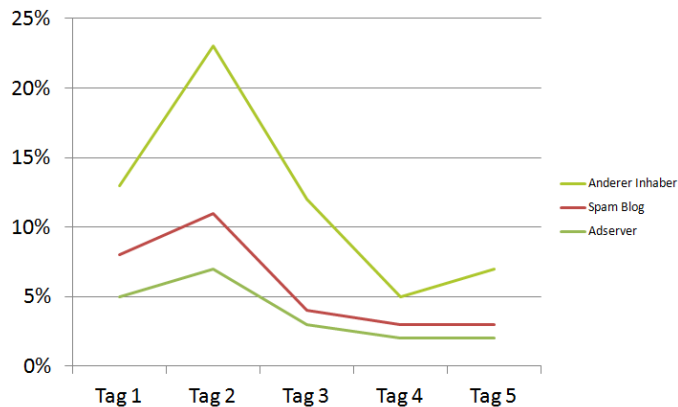
Flash:

Beim Flashcookie-Stuffing werden zum Cookiesetzen Flash-Objekte benutzt. Flash-Elemente (zum Beispiel YouTube-Videos) laden die Seite des Merchants im Browserhintergrund. Flashcookie-Stuffing ist nur äußerst schwierig zu identifizieren und man kann solche Cookies über aktuelle Filter so gut wie nicht deaktivieren.

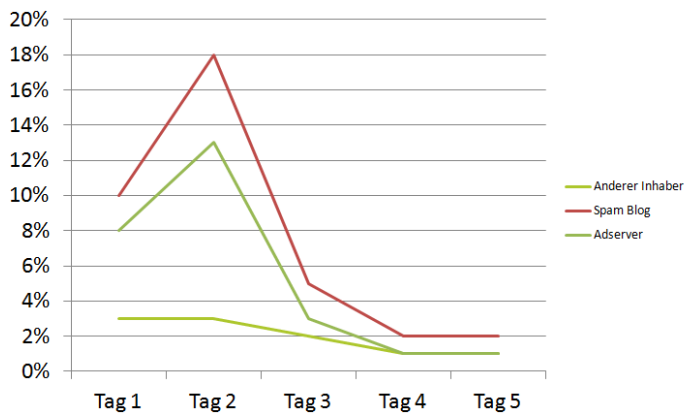
Anmeldung bei Affiliate Programmen über Netzwerke

Wir haben uns bei den bekanntesten Affiliate Programmen in Deutschland über verschiedene Affiliate Netzwerke beworben. Hierzu haben wir eine Internetseite mit einem anderen Impressum genommen, eine offensichtliche SPAM Seite, eine AdServer Startseite und themenspezifische Seiten.

Anmeldung erfolgreich



Anmeldung nicht erfolgreich



Viele Programme haben unser Anmeldung auch nach Wochen nicht angenommen, daher hier nur eine prozentuale Übersicht unserer Tests.

Sicherheitslücke entdeckt

Bei unseren Testläufen ist uns eine Sicherheitslücke aufgefallen, mit der es uns möglich ist, uns bei über 600 Programmen innerhalb von 3 Min. zu bewerben und die Trackingcodes zu erhalten.

Schnelltest: <http://www.cookie-monitoring.com/schnelltest.html>

Dem Merchant ist es bei der Sicherheitslücke weder möglich uns als Partner zu erkennen, identifizieren, noch nachzuvollziehen woher der Traffic kommt.

In unseren Testläufen haben wir uns mit einer E-Mail Adresse z.B. spam@spam.de , mit den Einstellungen, das wir Aktionsklicks machen, Adware betreiben und alle anderen möglichen Schweinereien machen, beworben und wurden trotzdem sofort automatisch freigeschaltet.

In unseren Statistiken liefen die generierten Sales und Leads als normale auf und wurden von den Merchants bestätigt. Die Zahlen finden Sie im Versuchsaufbau.

Verschleierung von Traffic

Nach dem wir die Trackingcodes von den Netzwerken erhalten hatten, haben wir Affiliates auf Verschleierungsmethoden überprüft, über jene Cookis Stuffing verschleiert werden kann.

IP Blocker - IP Tracking bei Anmeldung

Hierbei werden Netzwerke, Agenturen und Merchants mit statischen IPs identifiziert, indem Ihre IP-Adresse gespeichert wird und somit problemlos erkannt wird ob jemand von dieser IP-Adresse öfter auf die Website kommt.

Referrer Abfrage

Kommt der User von Goolge oder einer Kampagnenseite ist somit nachzuvollziehen, weil, wenn man einem Link von einer Seite folgt und auf diesen klickt wird im Normalfall ein sogenannter Referer mit an die neue Homepage gesendet. Dieser zeigt an von welcher Homepage der Surfer kommt.

Referrer Fake

Man kann die Herkunft des Traffics „faken“ bzw gänzlich „blanken“ (fake oder blank HTTP_REFERER). So können Betrüger Ihre Aktivitäten vertuschen.

Mouse Action

Bewegt sich die Maus auf dem Bildschirm kann der Affiliate von einem realen Besucher ausgehen.

Browser

Im Firefox kann man automatisiert Cookies setzen, dieses wird benutzt da die meisten Bots den IE Header nutzen.

Fingerprinting

Hierbei wird die IP und alle Browserinformationen gespeichert und aufbereitet um wiederkehrende Bots/Besucher auszuschließen. Hierzugehören neben Headerinformationen auch installierte Schriften, Sprachen, Plugins uvm.

Versuchsaufbau

Testzeitraum waren drei Monate (Jan-Mär 2011) in dem wir uns unangemeldet mit Accounts bei den Netzwerken und Affiliate Programmen beworben haben. Die Testaccounts wurden nach den Versuchen gelöscht und nicht ausbezahlt.

Versuch A)

- 6 Branchen mit jeweils 3 Partnerprogrammen
- 18 Trackingcodes nach Freigabe
- 1.000 Cookies bzw. Views/Tag mit
- 3 Cookies pro Impression
- Sichtbare Banner in der Größe 234x60
- Einbindung Trackingcode über Iframe
- CTR bei 1-4% mit Image Preloadern
- **Kein IP Blocker**
- **Keine Referrer Abfrage**
- **Keine Fake Referrer**
- **Kein Fingerprinting**
- Ergebnis: 1 von 18 Partnerprogrammen hat uns entdeckt
- 1 Partnerprogramm mit über **3000€ bestätigten (Verlust)**

Versuch B)

Trackingcodes aus der **Sicherheitslücke** auf 30 Programme aus verschiedenen Themengebieten:

- Zeitraum 1 Monat
- Einbindung Trackingcode über Iframe
- **Kein IP Blocker**
- **Keine Referrer Abfrage**
- **Keine Fake Referrer**
- **Kein Fingerprinting**
- 19.693 Klicks/Cookies
- 30.432 Views (Fehler im CTR Script)
- 20 Storno (90,61€)
- **283 Sales mit 1682,94 € bestätigter Provision**

Aussichten

Die Cookiestuffer schlafen nicht und entwickeln ständig neue Methoden ihre schadhaften Cookies unters Volk zu bringen. Man muss noch nicht einmal sonderlich technisch versiert sein, um Cookiestuffing betreiben zu können.

Für Anfänger in diesem Bereich gibt es mittlerweile sogar ein E-Book zu kaufen, in welchem Cookiestuffing Methoden erklärt werden. In einschlägigen Blogs sind die Codes für die Stuffingmethoden frei zugänglich für jeden und können einfach rauskopiert werden.

Die Geschädigten sind zum einen die ehrlichen Affiliates, da die Provisionen, die ihnen für ihre ehrliche Werbeleistung zusteht an Betrüger ausgezahlt wird, zum anderen die Merchants, die Provisionen für Verkäufe zahlen, die sowieso erfolgt wären.

Schützen Sie sich mit:



cookie-monitoring.com
Protect your Affiliate Marketing