

Guerilla Marketing

Werbung die auf den ersten Blick nicht als solche zu erkennen ist. Wird aktuell gerne genutzt um andere Communities zu infiltrieren und von deren Popularität und hohen Nutzerzahl zu profitieren.

Guerilla Marketing beschreibt Werbung die nicht als solche direkt zu erkennen ist. In Internet-Communities gilt es als besonders fiese Form des werbens ([Guerilla Spamming](#)). Hierbei werden scheinbar Hilfreiche Beiträge mit sichtbaren oder nicht gleich sichtbaren Verweisen auf die eigene Seite erstellt. Ziel ist es den Nutzer neugierig zu machen und so auf die eigene Webseite zu locken.

Ein weiterer Vorteil von [Guerilla Spamming](#) ist das manipulieren von Suchergebnissen in Suchmaschinen. [Searchbot Mining](#) nennt sich das. Hier wird die Popularität von erfolgreichen Communities genutzt um Suchmaschinen auf die eigene Seite aufmerksam zu machen. Erfolgreiche Communities werden von Suchmaschinen öfter besucht und alle dort gefundenen Link werden oft höher eingestuft.

Erstellt also ein unseriöser Webmaster in vielen großen Communities Beiträge, in denen er immer wieder auf seine Inhalte verweist z.B. durch [Deep-Linking](#), stuft die Suchmaschine seine Seite automatisch höher und wichtiger ein. Suchmaschinen berechnen nämlich den Rang einer Seite danach wie beliebt sie ist, und das ermittelt die Suchmaschine anhand daran wie viele Webseiten auf die Seite verweisen. Je mehr Webseiten also links zur Seite des Guerilla Spammers enthalten desto weiter oben steht er in den Suchergebnissen.

Ein Beispiel hier aus dem Forum:

Benutzer Anonymous posted einen Teil einer Story, unten drunter steht dann ein Link zu seiner Seite mit Satz "Die Fortsetzung gibt es hier, ich habe noch mehr schöne Geschichten"

Dies ist Guerilla Spam denn am Anfang sieht es nach einem normalen Benutzerbeitrag aus... erst unten wird klar das es ihm nur darum ging die Benutzer auf seine Seite zu locken.

Zweites Beispiel:

Ein Benutzer posted ein Paar Bilder, lädt diese aber nicht per Upload hoch sondern fügt sie als [Deep-Link](#) in seinen Beitrag ein. Die Bilder liegen auf seinem Webspace. Öffnet ein Benutzer das Bild wird er automatisch zur Seite den Spammers geleitet. Neugierige Benutzer kommen dann schnell auf die Idee die URL anzupassen um auf seine Hauptseite zu kommen in der der Erwartung weitere Bilder zu bekommen. Meistens ist es dann jedoch eine PaySite oder ein Onlineshop wo man Filme etc. kaufen soll.

Diese Form gilt als die fieseste da der Spammer immer behaupten kann das er das nicht wusste und ja nur gute tun wollte. Auch erkennen die meisten Benutzer ein per [Deep-Link](#) eingefügtes Bild nicht sofort. Der Spammer kann außerdem die Bilder auf seinem Webspace jederzeit austauschen und somit auch Schadcode auf den Rechner des Besuchers einschleusen, selbst wenn er keine "bösen" Absichten verfolgt spätestens wenn er seine Bilder löscht oder die Ordnerstruktur verändert, sind seine Beiträge nutzlos da die per [Deep-link](#) eingefügten Bilder nicht mehr angezeigt werden.