Report Juni 2014

„Non Human Traffic“ im Internet
S. 1-5

Gastkommentator - Dr. Bruno Glaus
Werbeauftraggeber müssen
WEMF vertrauen können
S. 6-7

mediatonic beginnt in der
deutschen Schweiz Fuss zu fassen
S. 8-9

Media Creativity
S. 10

mediatonic
integrated media thinking

„Non Human Traffic“ im Internet

Warnung vor falschen Internetnutzern

Laut einem im vergangenen Dezember* veröffentlichten Bericht machte der durch Roboter (Bots) generierte Traffic im Jahr 2013 60% des gesamten Verkehrs im Internet aus. Damit hat sich dieser Anteil im Vergleich zu 2012 um 20% erhöht. Hintergrund ist eine simple Tatsache mit komplexen Auswirkungen: Es ist im Web nicht immer einfach, Menschen und Bots zu unterscheiden.

Der schnelle Anstieg des nicht-menschlichen Traffics im Web hat die verschiedensten Ursachen. Nicht alle davon sind für das Online-Marketing problematisch. Der zunehmende Einsatz von Indexierungs-Roboter, die wachsende Zahl von Tools zur Optimierung der natürlichen Suchmaschinen-Referenzierung oder immer mehr digitale Überwachungssoftware: Die nicht-menschliche Aktivität im Internet nimmt immer mehr zu. Dabei bieten die betreffenden Programme dem Internetnutzer meist durchaus greifbare Vorteile. Es handelt sich um „gutmütige“ Spione, die es insbesondere Suchmaschinen ermöglichen, ihre Ergebnisse immer häufiger zu aktualisieren und immer bessere und aktuellere Ergebnisse zu liefern. Aber der im vergangenen Winter erschienene Bericht enthält auch warnende Töne: Auch der nicht-menschliche Verkehr durch bösartige Roboter, insbesondere durch „Hochstapler“, die sich im Netz als normale Internetnutzer ausgeben, ist sprunghaft angestiegen.

Jeder vierte Online-Aufruf stammt heute von einer Software, die sich als menschlicher Internet-nutzer tarnt.

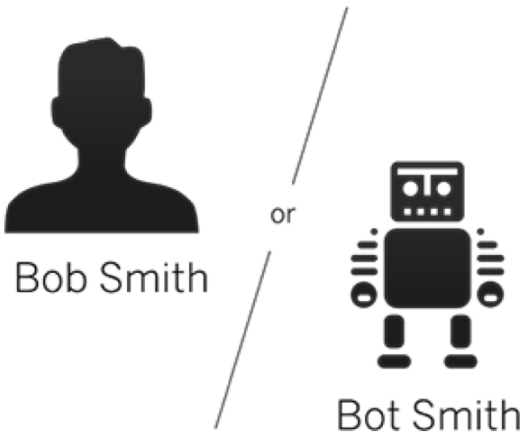
Für einen Adserver oder ein System zur Auswertung des Datenverkehrs besteht die einfachste Möglichkeit, non human Traffic herauszufiltern darin, aus seinen Statistiken alles zu löschen, das von in der „IAB/ABC International Spiders & Bots List“ erfassten Verursachern herrührt. Diese seit 2004 erscheinende Liste

* erschienen im Blog von Incapsula, einem auf dem Gebiet der digitalen Sicherheit tätigen Unternehmen, http://www.incapsula.com/blog/bot-traffic-report-2013.html

enthält eine aktuelle Zusammenfassung aller gutwilligen und böswilligen Bots und anderen „Datensammler" und steht allen Beteiligten der digitalen Lieferkette zur Verfügung. Damit lassen sich die Aktivitäten bekannter Roboter aus den Datenverkehrsstatistiken einer Website ebenso herausfiltern, wie jene aus den Statistiken einer Werbekampagne. Dieses einfache Verfahren versagt jedoch bei Bots, die ihre Identität verschleiern.

Nur durch eine Verhaltensanalyse des Datenverkehrs lassen sich solche Programme von Menschen unterscheiden. Anders ausgedrückt, man muss in der Art und Weise, wie sich ein Besucher im Web verhält, nach Auffälligkeiten suchen, die eine nicht-menschliche Aktivität nahelegen (Aufrufzyklen, wiederholte Klicks, wiederholter Aufruf von Websites usw.). Es ist leicht vorstellbar, wie kompliziert ein solches Vorgehen ist und welche grossen technischen Ressourcen für seine sinnvolle Durchführung erforderlich sind. Laut verschiedenen Schätzungen sind derartige identitätsverschleiernde Roboter heute für 20% bis 35% des weltweiten Internetverkehrs verantwortlich. Anders gesagt, mehr oder weniger jeder vierte Online-Aufruf ist heute auf ein Programm zurückzuführen, das sich als menschlicher Internetnutzer tarnt. Und bei alldem gibt es kein sicheres Mittel, diese Art des Internetverkehrs eindeutig zu erkennen.

Das IAB scheut sich mittlerweile nicht mehr, von einer regelrechten „Krise" durch betrügerischen Datenverkehr zu sprechen.



www.whiteops.com

Was aber steckt hinter diesen falschen Internetnutzern? Und welchen Sinn hat das Ganze?

Der Markt für Online-Werbung (Display-Advertising) umfasste alleine in den USA im vergangenen Jahr rund 13 Milliarden USD (Quelle: PwC). Ein Viertel dieser Investitionen wird heute automatisiert über Online-Marktplätze, Börsen für Ad Impressions oder Seitenaufrufe, den berühmten „Ad Exchanges", abgewickelt. Die Besonderheit dieses RTB/RTA-Auktionsverfahrens (Real Time Bidding/Advertising) besteht darin, dass nicht mehr ein spezielles Placement auf einer Website eingekauft wird. Vielmehr werden Aufrufe durch einen klar definierten Internet-Nutzertyp in dem Augenblick erworben, zu dem der betreffende Aufruf erfolgt. Oft kommt ein Biet-Agent zum Einsatz. Bei diesem Planungsprinzip geht es also weniger um den Ursprung des Traffics (die Website, auf der der Aufruf tatsächlich generiert wird), als um den reinen Werbeleistungswert und dessen Preis. Die wichtigste Rolle spielen hier ROI-Kennzahlen, auf deren Grundlage Algorithmen automatisch die betreffenden Käufe optimieren. Hinter alldem steht ein einfaches Ziel: Mit minimalem Investitionsaufwand sollen möglichst viele Aufrufe, Klicks oder Conversions erzielt werden.

Weltweit deutet alles darauf hin, dass der Anstieg der programmbasierten Käufe (RTA/RTB) mit dem des böswilligen nicht-menschlichen Verkehrs zusammenfällt. Es ist nicht schwer zu nachvollziehen, dass es in einem entmaterialisierten Einkaufsumfeld, in dem sich die Aufmerksamkeit weit stärker auf den Werbeleistungswert als auf den Ursprung des Traffic richtet, für die Urheber des entsprechenden Datenverkehrs finanziell sehr lukrativ sein kann, Aufrufe oder Klicks in grosser Zahl zu generieren.

Seit Anfang des Jahres hat die betreffende Kontroverse auch in den USA an Fahrt zugenommen. Das IAB scheut sich dort mittlerweile nicht mehr, von einer regelrechten „Krise" durch betrügerischen Datenverkehr zu sprechen. Der Verband hat in diesem Zusammenhang eine neue Taskforce ins Leben gerufen, deren Ziel es ist, das Problem des „non-intentional traffic" besser zu verstehen und in der Branche publik zu machen (siehe www.iab.net/fraud).

Whiteops, spider.io: Der Widerstand gegen die Roboter formiert sich

Die für betrügerische Zwecke eingesetzten Techniken werden immer ausgefeilter und haben im „Botnet" ihren vorläufigen Höhepunkt gefunden. Botnets sind mehr als einfache Programme zur Generierung von Aufrufen. Diese Netzwerke bestehen aus privaten Computern, die teilweise durch über Computerviren übertragene Software ferngesteuert werden. In den Vereinigten Staaten sind 15% des privaten Computerbestands mit Breitband-Internetzugang auf diese Weise „infiziert". Dadurch ist es möglich, reale Endgeräte ohne Wissen der Eigentümer dieser Geräte in erheblichem Umfang auf den durch den Betreiber des Botnets gewünschten Sites surfen zu lassen. Auch die Eigenschaften und Cookies der betreffenden Geräte sind dann natürlich echt. Solche „Zombie-Netzwerke" sind das klassische Werkzeug von Internet-Piraten, die DDoS-Angriffe starten wollen. Sie werden heute aber auch immer öfter für die genannten Betrügereien im Werbebereich verwendet.

Schätzungen des amerikanischen Spezialunternehmens Whiteops zufolge werden mit Online-Werbebetrug mittlerweile Umsätze von mehreren Milliarden Dollar erzielt. Sein CEO, Michael Tiffany, erklärte vor kurzem auf einer Konferenz des IAB anhand eines sehr einfachen Beispiels, weshalb dies unter Hackern derart in Mode gekommen ist: Eine gestohlene Kreditkartennummer erzielt auf dem Schwarzmarkt 25 Cents. Tausend durch ein Programm generierte Werbeseiten-Aufrufe bringen dagegen problemlos das Zehnfache ein – bei weit geringerem strafrechtlichem Risiko.

Was kann man in diesem unsicheren Kontext tun?

Ein anderer auf diesem Gebiet anerkannter Experte ist Douglas de Jager, Gründer von spider.io, das im vergangenen Februar durch Google aufgekauft wurde. Im Frühjahr 2013 war sein Unternehmen insbesondere massgeblich an der Aufdeckung des Botnets „Chameleon" beteiligt. Zum Zeitpunkt seiner Entdeckung im März 2013 generierte dieses Netzwerk rund 30% des über die wichtigsten amerikanischen Ad Exchanges angebotenen Werbeinventars. Und auch die Sites wichtiger Herausgeber waren betroffen. Das Botnet hatte die Kampagnen der grössten Marken sabotiert – Amex, Ford, BMW und auch McDonald's. Trotz des Ausmasses des Betrugs konnte bis zum heutigen Tag kein Verantwortlicher hinter „Chameleon" ermittelt werden.

Angesichts der zunehmenden Bedeutung dieses Phänomens werden Lösungen entwickelt, mit denen sich Fehlerrisiken und Betrug im Rahmen des Online-Verkehrs ausschliessen oder zumindest reduzieren lassen. Bislang scheinen die Betrüger allerdings noch einen erheblichen Vorsprung zu haben. Der Grund ist die Trägheit des Werbemarkts, dessen Mitspieler fürchten, den guten Ruf der „absoluten" Messbarkeit des Digitalen zu beschädigen und die rasant wachsenden Investitionen in die neuen Medien zu gefährden.

Adweek, Oktober 2013

Wie bereits gesagt, ist die Liste „Spider & Bot List" des IAB der erste Schritt für alle Beteiligten der digitalen Lieferkette. Nach unseren Erfahrungen offenbaren manche Adserver, die von wichtigen Publishers in der Schweiz genutzt werden, bereits in diesem Stadium Schwächen, da diese Liste nicht so oft aktualisiert wird, wie es eigentlich nötig wäre. Andererseits bieten gewisse Ad Exchanges noch immer Inventare an, die zu einem erheblichen Teil nicht-menschliche Agenten enthalten, welche auf der erwähnten Liste figurieren. An dieser Stelle ist es sinnvoll, bei den betreffenden Partnern auf der technischen und kommerziellen Seite sicherzustellen, dass zumindest diese mögliche Filterung aktiviert ist und von einer aktuellen Liste ausgegangen wird.

Auch die zur Verhaltensfilterung eingesetzten Technologien werden kontinuierlich weiterentwickelt. Sie sind ein weiterer unverzichtbarer Faktor für jeden verantwortungsbewussten Akteur im Ökosystem der Online-Werbung. Die Situation ist hier recht schwierig einzuschätzen, da die betreffenden Filterungstechniken naturgemäss geheim gehalten werden. Davon abgesehen hat aber jeder Werbekunde und jede Agentur das Recht, von seinem oder ihrem Partner die Offenlegung seiner Vorgehensweise hinsichtlich Verhaltensfilterung sowie der einzelnen Elemente, aus denen diese besteht, zu verlangen.

Die Bewertung der Sichtbarkeit der Werbemittel ist unserer Ansicht nach ein wesentliches Element für die Überwachung etwaiger Unregelmässigkeiten bei Durchführung einer Kampagne.

Hier unser Rat in Form eines Vierpunkte-Plans mit Massnahmen und Verhaltensweisen, mit denen dem zunehmenden nicht-menschlichen Verkehr und dem Betrugsrisiko im Internet begegnet werden kann:

1. Adserving durch Dritte: Bei einer Display-Kampagne ist es entscheidend, auf einen vom Anbieter der „Werbefläche" unabhängigen Adserver zurückzugreifen, um etwaige Betrugsprobleme zu entdecken. Andernfalls bleibt der Werbekunde hinsichtlich einer möglicherweise schwachen Filterung des „Non Human Traffic" durch den Herausgeber der Website oder hinsichtlich aller anderen Arten des Betrugs extrem angreifbar.

2. Erweiterte Möglichkeiten, nicht-menschlichen Datenverkehr zu filtern: Die Zertifizierung (zum Beispiel MRC) der in einer Adserving-Lösung zur Verfügung stehenden Metriken ist ein Element, das einen höheren Stellenwert erhalten sollte. Zudem wird die Fähigkeit einer Adserving-Lösung, nicht-menschlichen Verkehr zu erkennen – insbesondere den betrügerischen Einsatz von „Botnets" – wohl zu einem immer wichtigeren Kriterium bei der Auswahl der betreffenden Lösung.

3. Gesteigerte Wachsamkeit bei RTB/RTA-Aktivitäten: Bei programmbasierten Käufen in Echtzeit ist auf grösstmögliche Transparenz der gewählten Inventarquellen zu achten. Die Sichtbarkeit der Werbemittel muss systematisch bewertet werden können. Für Werbekunden, die in erheblichem Umfang über Ad Exchanges einkaufen, erscheint es mittlerweile sinnvoll, Betrugserkennungslösungen von Drittanbietern zu prüfen (zum Beispiel Peer 39 von mediamind/Sizmek).

4. Vorsicht bei der Definition automatischer Optimierungskriterien: Alle automatisierten Elemente innerhalb der Planungskette müssen mit grosser Vorsicht gehandhabt werden. Dies betrifft insbesondere Algorithmen, die sich im Betrugsfall widersinnig auswirken können – wie beispielsweise Algorithmen zur Optimierung der Verbreitung in Abhängigkeit von der Klickrate im Kontext einer Website mit vielen automatisch generierten Klicks. Im Übrigen sollten bei Kampagnen des Typs RTB/RTA so weit wie möglich automatische Optimierungen anhand leicht manipulierbarer Metriken wie Klicks oder Interaktionen vermieden werden. Stattdessen sollten die Zielvorgaben auf „echte" Conversions abgestellt werden. Der wichtige Punkt dabei ist, nicht ausschliesslich auf ein Preis/Leistungs-Verhältnis zu achten, sondern kritisch zu hinterfragen, welche Art Leistung tatsächlich erbracht wird.

Für das Web gilt noch mehr als für andere Kanäle, dass Zählen und Messen nicht identisch sind. Bei Besuchen, Impressions, Klicks oder Conversions handelt es sich nicht um „harte Tatsachen" sondern lediglich um Indikatoren, die sich aus einer Filterung und Auslegung gegebener Rohdaten ergeben. Angesichts der rasanten Zunahme böswilliger Akteure liegt es im ureigenen Interesse der Werbebranche, an geeignete Massnahmen zur Wahrung ihrer Glaubwürdigkeit zu denken und diese auch umzusetzen.

Matthieu Robert – Online Director
mediatonic SA

Werbeauftraggeber müssen WEMF vertrauen können

Von Dr. Bruno Glaus*

Die Basler Staatsanwaltschaft hat im Februar eine Untersuchung gegen die Wochenzeitschrift TagesWoche eingeleitet. Anlass waren anscheinend trotz WEMF-Beglaubigung überhöht angegebene Auflagenzahlen. Die Angelegenheit könnte Anlass geben, an den Kriterien einer derartigen Beglaubigung zu zweifeln, aber auch an den Kontrollmechanismen, die das Institut zur Prüfung ihrer Voraussetzungen einsetzt.

Im Zusammenhang mit der fragwürdigen Auflage-Frisierung der Basler „Tages-Woche" muss man erneut von einem Glaubwürdigkeitsverlust der WEMF AG für Werbemittelforschung sprechen. Erneut deshalb, weil der Fall „Giornale del Popolo" nur etwas mehr als 10 Jahre zurückliegt: Filippo Lombardi hatte zugegeben, die Auflagenzahlen des „Giornale" geschönt zu haben. Irritierend ist im jüngsten Fall die Verlautbarung der WEMF-Geschäftsführung, das Reglement sei unklar, die Beglaubigung der „TagesWoche" sei korrekt.

Tatsache ist: Das Reglement ist ziemlich klar: Zeitungen müssen (müssten!) im Impressum gemäss Ziffer 5.10 des Reglementes „die verbreitete Auflage und davon die verkaufte Auflage" angeben. Zwei Zahlen also. Ein Blick in die Schweizer Zeitungslandschaft genügt: Nur wenige Produkte halten sich an diese Vorgabe. Die WEMF hat nie interveniert. Sie macht geltend, eine Kontrolle der Zeitungsimpressen hätte „die Kapazitäten der WEMF überfordert" (sic!), so die WEMF-Geschäftsführung in der NZZ vom 11.3.2014.

* Der Schweizer Medien- und Werberechtsexperte Dr. iur. Bruno Glaus (www.glaus.com) ist Verwaltungsrat von mediatonic SA. Die NZZ vom 11.3.2014 hat die kritische Würdigung unseres Verwaltungsrats thematisiert.

Die verbreitete Auflage besteht aus der verkauften Auflage (Einzelverkauf und Abonnements inkl. max. 5% Gratisexemplare) sowie aus der darüber hinausgehenden Gratisauflage (Ziffer 5.9). Zur Gratisauflage zählen Gratisabonnements, Haushaltsstreuung, Selbstbedienung, Handverteilung und Zielgruppenversand (Ziffer 5.8).
Der TagesWoche-Deal mit der Vertriebsorganisation in den Flughäfen Zürich und Basel fällt unter die Kategorien Selbstbedienung und Handverteilung. Soweit verteilt! Es handelt sich zweifelsfrei um Gratisexemplare, welche nur beschränkt (max. 5 Prozent) der verkauften Auflage zugeteilt werden dürfen.

Sinngemäss wurde argumentiert, es handle sich um ein „Gegengeschäft". Diese Argumentation geht fehl. Ein Gegengeschäft liegt nur vor, wenn sich zwei in etwa gleichwertige Leistungen und Gegenleistungen gegenüberstehen. Der Vertrieb von 9'000 Exemplaren TagesWoche in den Flughäfen entspricht aber kaum mehr als 10 Prozent des normalen Abo-Preises. Trotzdem stellt die Vertriebsorganisation eine Gegenrechnung in der Höhe der Abonnements-Rechnung der „TagesWoche" für rund 9'000 Exemplare. Für welche Gegenleistung wohl?

Auch wenn das System auf Selbstdeklaration basiert - die WEMF kann sich nicht aus der Verantwortung stehlen. Würde es am Reglement liegen, hätte die WEMF dieses schon vor 10 Jahren, spätestens nach dem Fall „Giornale del Popolo", revidieren können und müssen. Auf die Frage „was könnte die WEMF verbessern?" hat ein Agenturvertreter gegenüber der Zeitschrift „persönlich" vor genau 10 Jahren geantwortet: „Die WEMF könnte die Kontrollen erhöhen". Wie wahr! Am Reglement liegt es nicht. Man muss es nur umsetzen. Und kontrollieren. Auch im Impressum der einzelnen Medien. Im Interesse der Werbetreibenden.

Dr. Bruno Glaus
VR mediatonic SA

_Interessantes aus der letzten Media.Research.Group-Studie

mediatonic beginnt in der deutschen Schweiz Fuss zu fassen.

Die Mediaagentur mediatonic ist in der Westschweiz die unbestrittene Nummer 1. Zwei von drei Werbeauftraggebern aus der Westschweiz sagen im letzten und in diesem Jahr in der von der Media.Research.Group* bei den Top750-Auftraggebern durchgeführten Werbemarkt-Studie, sie wüssten genau, wofür mediatonic steht, deren Leistungen seien ihnen sehr gut bekannt. Keine andere der 20 abgefragten Mediaagenturen kommt bezüglich Bekanntheitsgrad auch nur annähernd an mediatonic heran. MEC Mediaedge, die Mediaagentur mit dem zweitbesten Bekanntheitsgrad, erfreut sich gerade mal bei jedem fünften welschen Werbeauftraggeber der höchsten Bekanntheit.

mediatonic ist in der Westschweiz die meistbekannte Mediaagentur: zwei von drei welschen Werbeauftraggebern kennen mediatonic und seine Leistungen gut.

Damit werden die Ergebnisse der letztjährigen Umfrage auf eindrückliche Art bestätigt. Nur gerade 17% der welschen Werbeauftraggeber sagen, mediatonic sei ihnen überhaupt nicht bekannt. Alle andern Mediaagenturen sind bei mehr als der Hälfte aller welschen Werbeauftraggeber unbekannt.

Im Deutschschweizer Werbemarkt sieht die Situation für die Genfer mediatonic natürlich etwas anders aus. Die mit Abstand bekannteste Mediaagentur ist mediaschneider. 86 Werbeauftraggeber der deutschen Schweiz (37%) geben an, diese Agentur sehr gut zu kennen. Dahinter folgen OMD mit 22% und Mediaxis mit 14%.

* Im Rahmen der Werbemarkt-Studie Media.Research.Group (www.mediaresearchgroup.ch) werden die Top750-Werbeauftraggeber gebeten, die im Schweizer Werbemarkt operierenden Mediaagenturen zu beurteilen.

2013 sagten erst 13 Deutschschweizer Werbeauftraggeber, sie würden mediatonic sehr gut kennen, 2014 tun dies schon 22. Damit ist mediatonic bereits sehr nahe dran an der Agentur auf dem dritten Platz. Und dies will was heissen, nämlich als Agentur aus der Romandie auf dem Deutschschweizer Werbemarkt auf Augenhöhe mit den besten nationalen Agenturen um Akzeptanz, Bekanntheit und selbstverständlich Mandate zu kämpfen.

In der Deutschschweiz ist mediatonic schon die vierte meistbekannte Mediaagentur, obwohl sie seinen Sitz in Genf hat.

Chris Fluckiger, CEO
mediatonic SA

_Media Creativity

_JEANRICHARD

Die Uhrenmarke JEANRICHARD gibt mit Hochgefühl ihre Partnerschaft mit der „Patrouille des Glaciers“ bekannt. Seit Dezember prägt die Marke das Erscheinungsbild der ersten elektrisch angetriebenen Taxis in Zermatt. Die beiden in den Farben der Manufaktur und des Terrascope-Modells „Patrouille des Glaciers“, einer auf 100 Stück limitierten Ausgabe, lackierten Fahrzeuge sind echte Originale an diesem berühmten Ort, der den alpinen Skilauf wie kaum ein anderer versinnbildlicht.

_YALLO

Für die Mobile Prepaidkarte von yallo (für günstiges Telefonieren ins Ausland), wurde zur Erreichung der ausländischen Communities, in diesem Falle die Bau-Arbeitskräfte, Plakate in den Baustellen-Toiletten angebracht. Zudem wurde mit einem Augen-zwinkern auch die Botschaft des Werbemittels an den Werbeträger sprich an den Plakatierungsort angepasst.

mediatonic
integrated media thinking

1 place st-gervais
ch-1201 genf
tel. +41 22 365 20 20
www.mediatonic.ch
info@mediatonic.ch