AppNexus

Viral Content: Das erste Warnsignal für Ad Fraud

Michael Misiewicz
Manager, Data Science

Laura Yu
Associate Data Scientist

©2017 AppNexus Inc. Alle Rechte vorbe-

KURZFASSUNG

Als weltweit führende unabhängige Plattform für Werbetechnologie verzeichnet AppNexus täglich Hunderte Milliarden Impressions, aus jedem Winkel des digitalen Ökosystems kommend. Das hat zum Vorteil, dass unser Data-Science-Team mit dem Thema Ad Fraud vertraut ist und darauf entsprechend reagieren kann. Dieses Whitepaper geht auf einige Beobachtungen ein, die unser Team hinsichtlich Ad Fraud gemacht hat, gibt einen allgemeinen Überblick über den aktuellen Status in der digitalen Medienlandschaft und liefert Empfehlungen für Publisher, Werbetreibende und Internetnutzer.

Hier sind einige der Highlights:

Ad Fraud stellt eine existenzielle Bedrohung für programmatische Werbung dar. Es kostet Werbetreibende nicht nur Milliarden von Dollar pro Jahr, sondern untergräbt auch das Vertrauen von Marken in den programmatischen Markt. Einem aktuellen Bericht des Chief Marketing Officer Council und Dow Jones zufolge haben 72 % der programmatischen Werbetreibenden Bedenken bezüglich Brand Safety und Kontrolle auf dem programmatischen Markt.

Anbieter für Traffic-Akquise bedürfen einer genauen Überprüfung. Urheber von viralen Inhalten sind besonders anfällig für Ad Fraud, wenn sie Traffic von fragwürdigen Drittanbietern erhalten. Um Betrug zu eliminieren, müssen Werbetreibende und Publisher die Traffic-Akquisefirmen in ihren programmatischen Supply Chains untersuchen.

Virale Inhalte gehen Hand in Hand mit Ad Fraud. Die Experten von AppNexus haben beobachtet, dass Publisher, die sich auf virale Inhalte spezialisieren, generell sehr viel häufiger nicht-menschlichen Traffic erhalten. Wir haben diesen Zusammenhang mithilfe von Data-Science-Methoden ermittelt, mit denen sich verdächtige Traffic-Muster und Überschneidungen bezüglich der Zielgruppen dieser Websites sowie der von ihnen erstellten Inhalte aufzeigen lassen. Unsere Analyse legt den Schluss nahe, dass viele dieser Websites von denselben Personen betrieben werden.

„Fake News“ und Volksverhetzung sind oft nur eine weitere Form von viralen Inhalten. Wir haben darüber hinaus einen Zusammenhang zwischen viralen Publishern und den „Fake News“ sowie extremistischen politischen Inhalten verzeichnet, die die öffentliche Debatte in den Monaten vor und nach der US-Präsidentschaftswahl 2016 dominierten. Genauer gesagt hat es den Anschein, als seien viele der werbefinanzierten Websites in diesen Kategorien gleichermaßen finanziell wie ideologisch motiviert. Unabhängig davon, welcher Faktor überwiegt, besteht eines der Hauptziele für den Großteil dieser Websites darin, möglichst viel günstigen Traffic anzuziehen, um ihre Profite aus Werbeeinnahmen zu steigern.

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

INHALTSVERZEICHNIS

1. Einleitung 4

2. Der Status von Ad Fraud 5

3. Grundlagen der Traffic-Akquise 9

4. Der Weg in die Zukunft: Ad Fraud bekämpfen 14

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

EINFÜHRUNG

In der digitalen Medienlandschaft gibt es kaum einen Trend, der für so viel Diskussionsstoff gesorgt hat wie der Anstieg „viraler" Inhalte.

Auch wenn diese Geschichten vielerlei Formen annehmen, sind sich Branchenbeobachter generell einig, dass gewisse Übereinstimmungen vorliegen. Im Großen und Ganzen ist ein viraler Inhalt eine leicht konsumierbare Geschichte, die darauf ausgelegt ist, in sozialen Medien geteilt zu werden. Von ideologisch voreingenommenen „Fake News" bis hin zu Videos von kranken Hunden, die auf die Tränendrüse drücken sollen – diese Geschichten zielen auf psychologische Trigger ab, um die Zuschauer zu manipulieren und sie in einen stark emotionalen Zustand zu versetzen.

Seit Jahren diskutieren Experten den Einfluss, den virale Inhalte auf das Online-Erlebnis und den politischen Diskurs in der ganzen Welt haben. Doch bisher haben die meisten von uns die Tatsache übersehen, dass die Anbieter viraler Inhalte in vielen Fällen **von Ad Fraud profitieren**.

Denn ohne einen stetigen Zustrom an Usern auf ihrer Homepage verzeichnen Publisher, die von viralem Social Traffic abhängig sind, erhebliche Höhen und Tiefen in ihren Umsatzkurven. Wenn eine Geschichte in den sozialen Medien einschlägt, läuft das Geschäft gut. Aber wenn ihre Inhalte bei sozialen Zielgruppen keinen Anklang finden, sind diese Publisher versucht, Traffic von Drittanbietern zu erwerben, die nicht immer legitim sind.

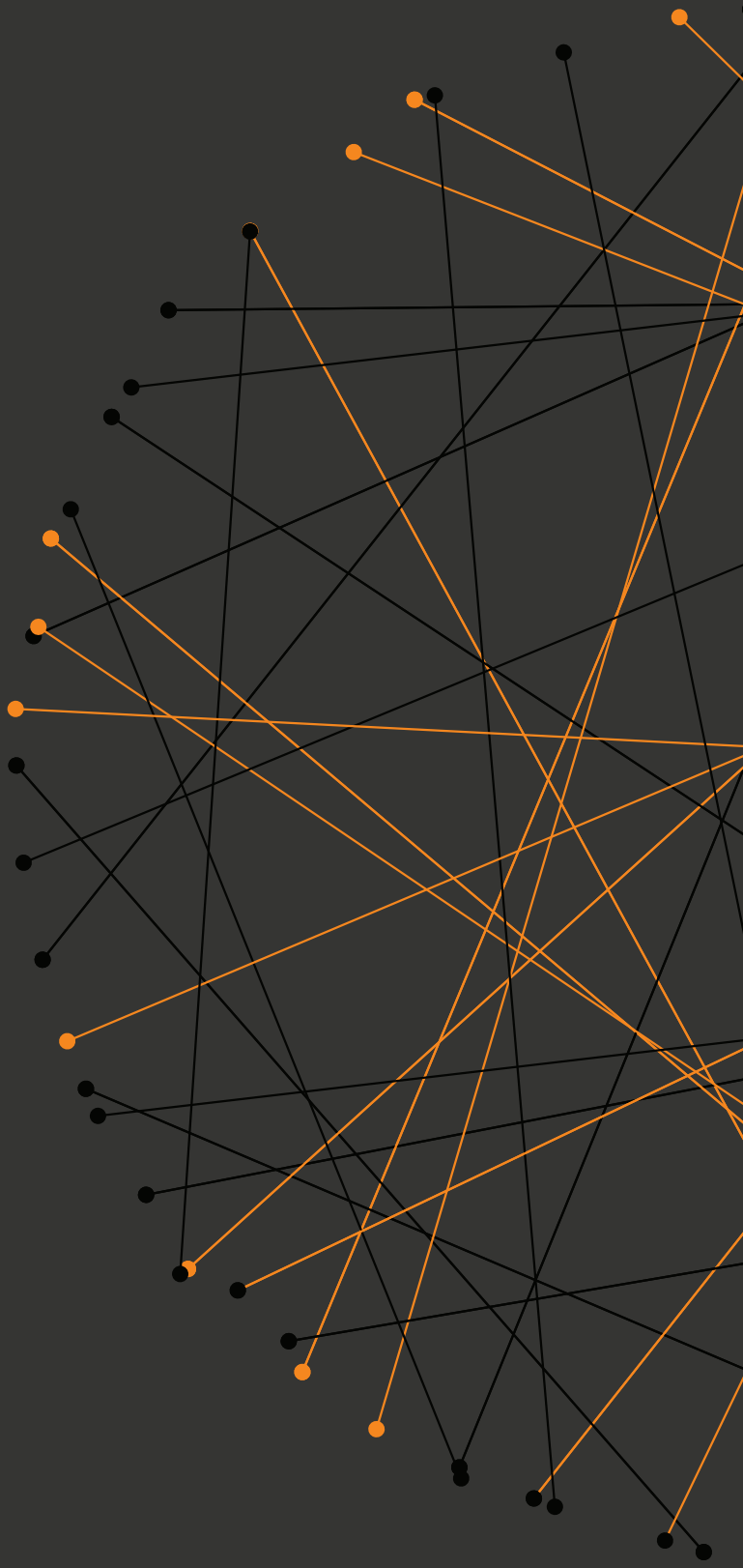
Im Rahmen unserer Beobachtung des Ökosystems für digitale Werbung haben wir festgestellt, dass virale Inhalte mittlerweile ein **Warnsignal** dafür geworden sind, dass ein Publisher wissentlich oder unwissentlich betrügerischen Traffic für sich selbst erwirbt oder nicht-menschliche User auf andere Seiten weiterleitet, um konstante (und wachsende) Umsatzziele zu erreichen. In diesem Whitepaper gehen wir näher auf unsere Erkenntnisse ein – in der Hoffnung, deutlich zu machen, was diese für die digitale Medienbranche und die Gesellschaft im Allgemeinen bedeuten.

Im Folgenden lesen Sie, was virale Inhalte auszeichnet, warum Publisher diese produzieren und wie böswillige Beteiligte diese nutzen, um betrügerischen Traffic zu erwerben und zu verkaufen. Darüber hinaus gibt dieses Whitepaper Werbetreibenden, Publishern und Technologieanbietern praktisch umsetzbare Ratschläge für die Bekämpfung von Ad Fraud an die Hand. Abschließend betrachten wir, was wir über Fake News und Volksverhetzung gelernt haben, und geben Aufschluss darüber, warum werbefinanzierte Publisher, die diese Art von Inhalten produzieren, wahrscheinlich nicht ausschließlich ideologisch motiviert sind.

Aber bevor wir zu alledem kommen, sollten wir einen Schritt zurückgehen und uns mit dem aktuellen Status von Ad Fraud vertraut machen.

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

DER STATUS VON AD FRAUD



Wie er passiert, wie er sich weiterentwickelt und was wir tun, um ihn zu stoppen:

Im Kern ist die Geschichte des Ad Frauds ein Katz-und-Maus-Spiel zwischen den „Bösen“ und denen von uns, die darum bemüht sind, ihnen einen Strich durch die Rechnung zu machen. Jedes Mal, wenn Marken, Publisher und Vendoren eine neue vorbeugende Maßnahme implementieren, entwickeln Betrüger eine noch raffiniertere Methode, um Werbebudgets einzustreichen, die für legitime, menschliche Zielgruppen bestimmt waren.

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

Auch wenn Betrüger bei diesem Diebstahl auf eine Vielzahl an Taktiken zurückgreifen, besteht der gemeinsame Nenner darin, dass sie vom Verkauf gefälschten Web-Traffics unter Vortäuschung falscher Tatsachen profitieren. In vielen Fällen gehört zu diesen Systemen, dass Marken und/oder Publisher für den Zugang zu Zielgruppen zahlen müssen, die in Wahrheit gar nicht existieren. Auch wenn ständig neue Methoden zum Einsatz kommen, finden Sie hier eine Liste der aktuell verbreitetsten Betrugsmethoden:

- **Browser- oder Device-Hijacking-Programme:** Malware, die die Kontrolle über den Browser eines Benutzers übernimmt und bestimmte Websites ohne das Wissen des Benutzers aufsucht.
- **Bot Netzwerke:** Server-basierte Browser, die vorgeben, menschliche User zu sein – diese Taktik wurde in den letzten Jahren mehr angewandt, als die oben beschriebene Browser-Hijacking-Malware.

- **Ad-Stuffing:** eine Taktik, bei der der Publisher unsichtbare Werbeanzeigen auf einer Website implementiert, die der Benutzer nicht sehen kann.

Es ist unmöglich, genau zu beziffern, wie viel Geld unehrliche Publisher sich unter den Nagel gerissen haben, doch das Interactive Advertising Bureau (IAB) schätzt, dass Ad Fraud unsere Branche im Jahr 2015 ca. 8,2 Milliarden USD gekostet hat. Das Werbeverifizierungs-Unternehmen Adloox hingegen sagt voraus, dass diese Kosten sich für 2017 auf bis zu 16,4 Milliarden USD belaufen könnten. Diese Werte sind von Natur aus ungenau, da es keinen eindeutigen, garantierten Indikator dafür gibt, dass eine Impression betrügerisch ist – doch diese Schätzungen machen deutlich, dass dies ein gewaltiges Problem für unsere Branche darstellt.

Neben den finanziellen Ausmaßen dieses Diebstahls stellt Betrug außerdem eine existenzielle Bedrohung für das digitale Ökosystem dar, da er das Vertrauen von Marken in den programmatischen Markt untergräbt. Laut eines aktuellen Berichts des Chief Marketing Officer Council und Dow Jones haben 72 % der programmatischen Werbetreibenden Bedenken bezüglich Markensicherheit und Kontrolle auf dem programmatischen Markt.

Wie eine komplexe Supply Chain Betrüger schützt

Wenn so viel auf dem Spiel steht, liegt die Frage nahe, warum noch niemand eine Lösung entwickelt hat, um Werbebetrug zu eliminieren und das Katz-und-Maus-Spiel ein für alle Mal zu beenden. Die Antwort liegt in der Komplexität der programmatischen Versorgungskette, einem vielschichtigen Ökosystem, das Marc Pritchard, CEO von Procter & Gamble, mit den berühmten Worten „bestenfalls undurchsichtig und schlimmstenfalls betrügerisch“ beschrieb.

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

Bei jeder programmatischen Transaktion sind Marken durch eine Vielzahl von Agenturen, Technologieanbietern und Werbenetzwerken vom Endbenutzer getrennt – und all diese liefern entscheidende Informationen über die Impressions, die die Marke kauft. Bei so vielen Sprüngen entlang der Kette kann es für alle an der Transaktion Beteiligten extrem schwierig sein, zu gewährleisten, dass der Rest ihrer Geschäftspartner ethisch korrekt handelt. Es braucht nur einen betrügerischen Beteiligten, um einen millionenschweren Diebstahl am Laufen zu halten.

Erst kürzlich deckte Buzzfeed ein solches System auf, bei dem eine digitale Medienagentur Device-Hijacking-Software nutzte, um Millionen von unechten Besuchern in ein Netzwerk minderwertiger Websites zu schleusen. Im Rahmen dessen gelang es der Agentur, aus den Werbebudgets von Disney, Gilette und über 100 weiteren Marken zu stehlen.

Was AppNexus für einen sauberen Marktplatz tut

Trotz aller Hindernisse, die uns im Weg stehen, hat AppNexus sich voll und ganz dem Ziel verschrieben, dem Werbebetrug ein Ende zu setzen und einen vertrauenswürdigeren digitalen Markt zu schaffen.

Im Laufe der letzten drei Jahre haben wir erhebliche Mengen an Zeit, Geld und Ressourcen investiert, um den Betrügern, die unsere Kunden gefährden, einen Schritt voraus zu bleiben. Heute haben wir zu jeder Zeit 30 Betrugsdetektoren laufen. Indem wir alle Daten im Zusammenhang mit jeder Impression sammeln – von dem Moment, wenn der Benutzer eine Seite öffnet, bis zu dem Moment, wenn die Anzeige erscheint –, können wir sehen, wenn etwas nicht stimmt. Darüber hinaus scheuen wir keinen Aufwand, um besser zu verstehen, wie Betrug funktioniert, indem wir die Malware, die die Betrüger verwenden, in einer sicheren „Sandbox"-Forschungsumgebung analysieren. So können wir sehen, wie die Malware sich bei ihren Versuchen verhält, menschliches Verhalten zu imitieren, und können verfolgen, welche Seiten sie aufruft, wodurch wir wiederum feststellen können, dass diese Websites mit hoher Wahrscheinlichkeit nicht-menschlichen Traffic kaufen.

Und das ist erst der Anfang. Als weltweit führende unabhängige Plattform für Werbetechnologie verzeichnen wir täglich Hunderte Milliarden Impressions, die allesamt von unseren Anti-Betrugs-Detektoren protokolliert und analysiert werden. Um die nächste Generation von Betrügern auszumerzen, haben wir uns entschieden, unsere einzigartige Perspektive zu nutzen, um zu erforschen, wo Betrug heute auftritt und welche neuen Taktiken eingesetzt werden, um die Budgets von Werbetreibenden zu stehlen.

Diese Fälle zu ermitteln und die Schuldfrage zu klären, ist nicht leicht, da es keinen einzelnen, definitiven Indikator dafür gibt, dass eine Impression betrügerisch ist. Aber mithilfe der neuesten maschinellen Lernverfahren können unsere

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

Datenwissenschaftler Trends und Muster finden, die mit hoher Wahrscheinlichkeit auf betrügerische Aktivität hindeuten. Zu diesen Verfahren gehören:

- **Cluster-Analyse:** ein grundlegendes Datenanalyseverfahren, bei dem Datenpunkte auf Grundlage wesentlicher Gemeinsamkeiten gruppiert werden. Cluster-Analysen helfen beim Aufspüren verdächtiger Gemeinsamkeiten zwischen Impressions, die von dubiosen Traffic-Quellen generiert werden.
- **Covisitation:** ein Verfahren, mit dem Überschneidungen des Traffics zwischen verschiedenen Websites identifiziert werden, was uns dabei hilft, Verbindungen zwischen Websites zu ermitteln, die fragwürdigen Traffic aus denselben Quellen erhalten. Diese Studie von Forschern an der NYU und Dstillery (vormals Media6Degrees) liefert eine tiefergehende Erklärung dafür, wie Covisitation Fälle von Werbebetrug aufdecken kann.
- **Honeypots:** ein Verfahren, bei dem wir Bots enttarnen, indem wir eine falsche Website erzeugen und dann Traffic von verdächtigen Anbietern auf diese senden. Wir können diesen dann auf Zeichen nicht-menschlicher Besucher analysieren.

Mithilfe dieser Verfahren hat unser Data-Science-Team ermittelt, dass Betrüger auf immer ausgefeiltere Taktiken zurückgreifen, um Mechanismen zur Betrugserkennung zu überlisten. Und, was womöglich am interessantesten ist, sie haben außerdem eine bedeutende Schnittmenge zwischen viralen Inhalten – einschließlich der Unterkategorien Fake News und Volksverhetzung – und betrügerischer Aktivität aufgedeckt.

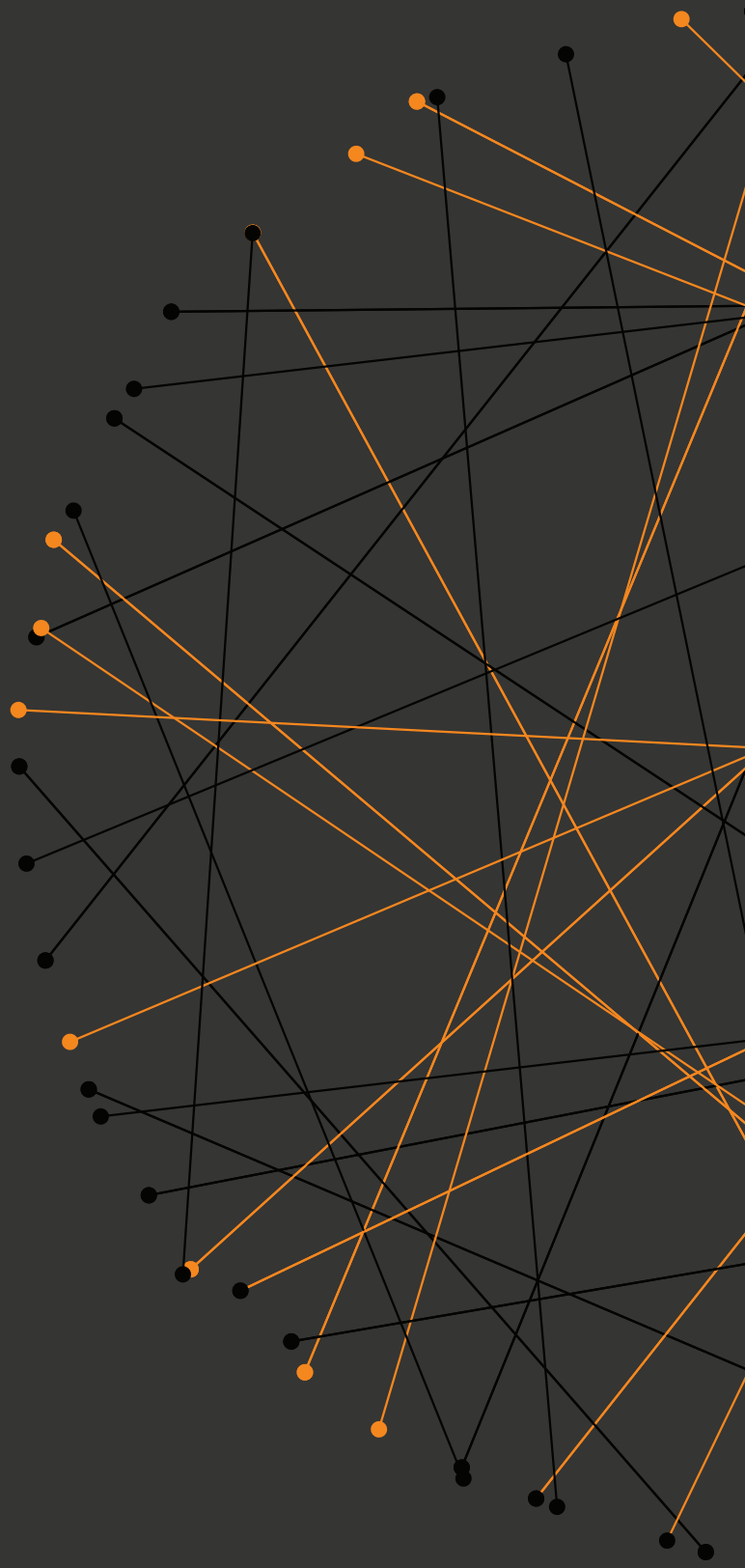
Warum Websites mit viralen Inhalten besonders anfällig für Betrug sind

Auch wenn nahezu alle großen Medienunternehmen zumindest mit Geschichten experimentieren, die auf soziale Medien ausgerichtet sind, ist die Wahrscheinlichkeit am höchsten, dass Publisher, die ihr gesamtes Unternehmen auf virale Inhalte aufgebaut haben, an betrügerischen Aktivitäten beteiligt sind. Neben ihrem Schwerpunkt auf Viralität stechen diese Publisher insofern hervor, als sie mit höherer Wahrscheinlichkeit finanziell motiviert sind – oder zumindest mit dreisteren Mitteln Profite verfolgen – als Medienunternehmen.

Im Wesentlichen nutzen virale Publisher die psychologischen Trigger teilbarer Inhalte, um innerhalb kurzer Zeit Zuschauerzahlen zu erreichen, für die herkömmliche Publisher Jahre brauchen würden. Indem sie die Vorliebe der Nutzer für niedliche Tiere, ihre politischen Unterschiede und ihr Festhalten an extremen Ideologien manipulieren, haben einige dieser Unternehmen ihre Inhalte mit großem Erfolg in sozialen Medien verbreitet. Und es kommt noch besser (für die Betrüger): Sie erzielen Werbeeinnahmen aus minderwertigen Beiträgen, die weitaus weniger Ressourcen erfordern als ein Nachrichtenbeitrag mit sorgfältiger Berichterstattung oder ein professionell produziertes Video.

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

GRUNDLAGEN DER TRAFFIC-AKQUISE



Natürlich sind nicht alle Traffic-Akquise-Geschäfte betrügerischer Art; um genau zu sein, sind viele von ihnen völlig legitim. Ohne Zweifel gibt es Tausende von Direct-Response-Brands, die Cost-per-Click-Anzeigen kaufen, um auf effektive Weise reale Benutzer auf ihre Produktseiten zu leiten. Aber generell lässt sich festhalten: Je weniger Sie für Traffic bezahlen, desto riskanter ist der Anbieter, mit dem Sie arbeiten, und desto geringer ist die Wahrscheinlichkeit, dass Sie echte Besucher auf Ihrer Website erhalten.

Es sind die trüben Gewässer zwischen einem vollkommen legitimen Cost-per-Click-Werbedeal und einem offensichtlich betrügerischen Botnetz, wo es kompliziert wird.

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

Hier finden Sie einen Überblick darüber, was wir als die drei wesentlichen Kategorien für Traffic-Akquise-Strategien betrachten – aufgeschlüsselt nach dem Betrugsrisiko, das diese darstellen.

Generell für sicher erachtet

Auch wenn es uns unmöglich ist, zu garantieren, dass ein bestimmter Kauf von Onlinewerbung zu 100 % betrugsfrei ist, so gibt es doch bestimmte Arten von Traffic-Akquise, bei denen Marken und Publisher sich darauf verlassen können, dass diese reale, menschliche Benutzer liefern. Dazu gehören:

- **Organische Marketing-Initiativen:** Die sicherste Option, um Traffic zu erzielen, ist die althergebrachte Methode – hervorragende Inhalte produzieren und auf deren Grundlage ein Publikum aufbauen. Die Quellen in dieser Kategorien sind u. a.:
  - **Direkter Traffic:** Traffic, dessen Ursprung ein menschlicher Benutzer ist, der schlicht und einfach die URL einer Website in seinen Browser eingibt.
  - **Organischer Such-Traffic:** Traffic, der von menschlichen Benutzern stammt, die eine Website in den nicht-gesponserten Ergebnissen einer Suchmaschine finden.
  - **E-Mail-Marketing**: Traffic, der generiert wird, indem eine E-Mail an eine Adresse gesendet wird, die ein menschlicher Benutzer dem Publisher mitgeteilt hat.

  Keine dieser Taktiken erzeugt garantiert ausschließlich sauberen Traffic, da es nach wie vor möglich ist, dass raffinierte Betrüger Bots erstellen, die das menschliche Nutzerverhalten simulieren, das mit der jeweiligen Form einhergeht. Aber das entscheidende Unterscheidungsmerkmal besteht darin, dass in jedem Fall der Publisher nicht für den Traffic bezahlt, weshalb es keinen Anreiz gibt (außer natürlich für den Publisher selbst), diesen auf betrügerische Weise zu erzeugen.
- **Pay-per-Click mit Suchmaschine:** Bei einem Pay-per-Click-Geschäft mit einer Suchmaschine erwerben Werbetreibende das Recht, einen Link in den Suchergebnissen eines Benutzers zu bewerben, nachdem dieser Benutzer eine Suchanfrage gestellt hat. Die führenden Suchmaschinen – d. h. Google und Bing – werden von großen, angesehenen Unternehmen mit eigenen Betrugsabteilungen betrieben, sodass Käufer, die mit ihnen arbeiten, sich darauf verlassen können, dass sie hochwertigen Traffic erhalten. Dasselbe lässt sich jedoch nicht von vielen der kleineren Anbieter in dieser Branche sagen.

  Unternehmen, die Pay-per-Click-Kampagnen in Suchmaschinen betreiben, stammen größtenteils aus dem Einzelhandel und nicht aus dem Publishing-Gewerbe. Wenn sie Zugang zu bestimmten Benutzern und Stichworten kaufen, zielen sie darauf ab, Produkte und Dienstleistungen zu verkaufen, wenn der Link angeklickt wird. Und da viele Einzelhändler von beträchtlicher Größe auf diesen

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

beliebten Suchmaschinen um Benutzer konkurrieren, sind die Kosten für bestimmte Stichwörter relativ hoch. Diese Kosten bedeuten, dass es praktisch nie profitabel ist, führende, hochwertige Suchmaschinen für Werbe-Arbitrage zu nutzen.

Darüber hinaus können diese Websites bestätigen, dass der Benutzer ein realer Mensch ist, wenn dieser einen Einkauf tätigt, da er gewisse Kontaktinformationen angibt, die erforderlich sind, um den Austausch von Waren und/oder Dienstleistungen abzuschließen. Auch wenn es möglich sein mag, eine E-Mail-Adresse oder Postanschrift zu fälschen, würde das Tätigen eines Einkaufs voraussetzen, dass ein Bot ausgefeilt genug ist, um ein Checkout-Verfahren zu durchlaufen, was mehr Zeit und Ressourcen in Anspruch nehmen würde, als die meisten Betrüger zu investieren gewillt sind. Und außerdem müssten Sie dann Geld für einen Artikel ausgeben, was wiederum sämtliche durch die Impression erzielte Werbeeinnahmen zunichte machen könnte.

Völlig betrügerisch

Es gibt einige Traffic-Akquise-Systeme, die Publisher vollkommen meiden sollten – und das aus offensichtlichen Gründen.

- **Cloudbots und Traffic-Austausch:** Bei dieser Art von Traffic-Akquise-Geschäft mietet ein Betrüger einen virtuellen privaten Server von einem Cloud-Hosting-Dienst wie Amazon Web Services, Server Beach oder Digital Ocean. Er lässt daraufhin einen automatisierten Headless-Browser laufen und besucht mehrere Websites, entweder direkt oder über einen Traffic-Austausch. Der virtuelle private Server kann vom Publisher selbst erstellt werden, oder der Publisher kann einen Dritten bezahlen, um ihm den Bot-Traffic zu senden.

  Bei einem Traffic-Austausch vereinbart eine Gruppe von Personen, die Websites der jeweils anderen vielmals aufzusuchen, um so ihren Traffic künstlich zu steigern. Dabei handelt es sich um betrügerische Aktivität, selbst in Fällen, in denen Publisher manuell zu den Websites ihrer Mitverschwörer navigieren.

  Als AppNexus 2015 eine Großinitiative startete, um Betrüger auszumerzen, kam der Großteil der Impressions, die wir über unsere Plattform terminierten, von Cloudbot- und Traffic-Austausch-Systemen. Doch die Betrüger haben neue Taktiken entwickelt, um nicht entdeckt zu werden. Letztes Jahr stahlen die Drahtzieher hinter dem Methbot-Betrug Berichten zufolge Millionen von Dollar, indem sie Rechenzentren als individuelle Nutzer von Heimcomputern maskierten (dank unserer fortwährenden Investitionen in Inventarqualität und Betrugserkennung war AppNexus kaum von diesem Angriff betroffen.)

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

Lassen Sie Vorsicht walten

Den Fokus dieses Whitepapers bildet die Grauzone, die zwischen sicherer Traffic-Akquise und offensichtlich betrügerischen Systemen liegt.

Während diese Verfahren zur Traffic-Akquise im heutigen Werbetechnologie-Ökosystem sowohl legal als auch zulässig sind, lassen sie einige Alarmglocken läuten und erfordern daher genauere Nachforschungen. Publisher, die auf diese Taktiken setzen, müssen vorsichtig sein, wenn es auch in Zukunft für sie bergauf gehen soll.

- **Content-Discovery-Netzwerke:** Firmen in dieser Kategorie bewerben Links zu Publisher-Inhalten in nativen Werbe-Widgets auf Websites im gesamten Web. Mittlerweile sind die meisten Menschen mit diesen Empfehlungs-Widgets vertraut, die sich in der Regel am Seitenende befinden.

  Obwohl diese Unternehmen mit einer Vielzahl legitimer Publisher arbeiten, kann es schwierig für Kunden sein, zu ermitteln, wie viel menschlichen Traffic sie wirklich erhalten. Selbst gewissenhafte Publisher können unwissentlich nicht-menschliche Benutzer über diese Programme kaufen, sofern mindestens eine andere Website im Netzwerk betrügerischen Traffic erworben hat.

  Wenn ein kleiner Publisher nur einen Teil seiner Content-Discovery-Daten sieht, kann es schwierig sein, zu ermitteln, wenn eine andere Website eine Kombination aus menschlichen und nicht-menschlichen Benutzern liefert.

- **Pay-per-Click in sozialen Medien:** Ein Pay-per-Click-Kauf für soziale Medien liegt vor, wenn ein Publisher eine Plattform wie Facebook oder Twitter dafür bezahlt, dass diese Links zu nativen Inhalten mitten im Feed von Benutzern platziert werden.

  Aufgrund des Preisspektrums für Werbung in sozialen Medien und der stetigen Veränderungen an den Newsfeed-Algorithmen sozialer Netzwerke müssen Arbitrageure ihre Strategie anpassen, um von diesem Kanal zu profitieren. In Fällen, in denen Werbung teuer ist, kann eine Website möglicherweise Geld verlieren, wenn sie einer Person eine Anzeige präsentiert, es sei denn, die Seite ist überladen mit Anzeigen. Doch in den meisten Fällen nehmen Publisher den Verlust durch einen individuellen Klick hin, in der Hoffnung, dass der Benutzer den Artikel mit seinem Netzwerk teilt und organischen Traffic aus sozialen Medien anzieht.

  Das ist einer der Gründe, weshalb soziale Medien so oft mit sonderbaren, gelegentlich sogar schockierenden Inhalten gefüllt sind. Die Websites haben kein Interesse daran, mit hoher Qualität ein langfristiges Publikum aufzubauen, und entscheiden sich stattdessen für schnelle und einfache Klicks. Somit greifen sie zu übermäßig dramatischen „Clickbait“-Titeln, um die Wahrscheinlichkeit zu steigern, dass Benutzer die Seite besuchen und ihre viralen Inhalte teilen.

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

Qualitätskontinuum für Traffic-Quellen

SICHER/HOHE QUALITÄT

Organische Traffic-Akquise	**Generell für sicher erachtet**
Pay-per-Click in Suchmaschinen	
Organisch in sozialen Medien	
Pay-per-Click in sozialen Medien	**Lassen Sie Vorsicht walten**
Content-Discovery-Netzwerke	
Cloudbots und Traffic-Austausch	**Völlig betrügerisch**
Pay-per-Click-Börsen und Botnets	

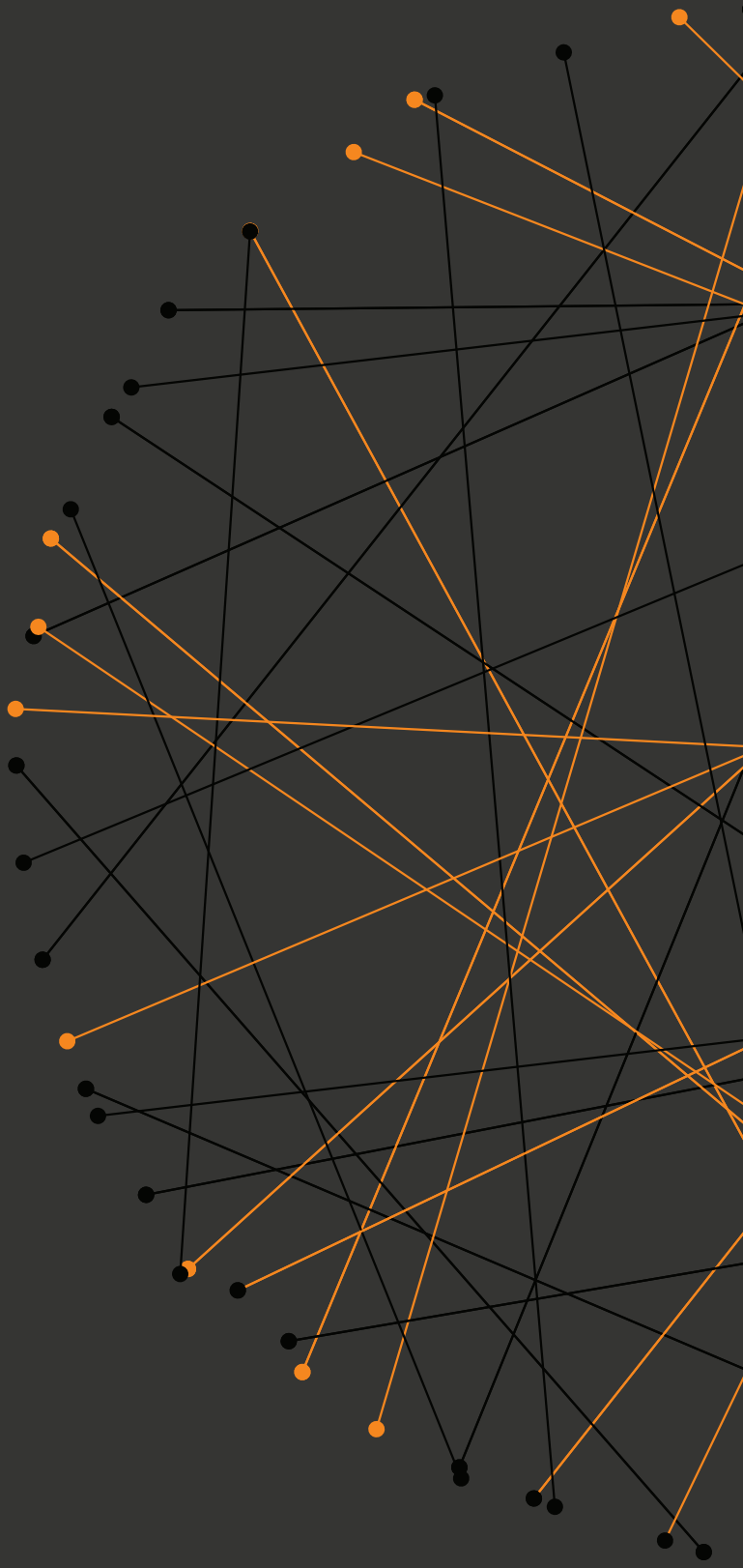
ÜBERAUS RISKANT/GERINGE QUALITÄT

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

DER WEG IN DIE ZUKUNFT

Werbebetrug im Zeitalter viraler Inhalte bekämpfen

Ein wichtiger Faktor, den man sich vor Augen führen sollte, ist die Tatsache, dass virale Inhalte lediglich die aktuellste Front in einem fortwährenden Kampf zwischen Betrügern und Betrugsbekämpfern darstellen.



 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

Ein wichtiger Faktor, den man sich vor Augen führen sollte, ist die Tatsache, dass virale Inhalte lediglich die aktuellste Front in einem fortwährenden Kampf zwischen Betrügern und Betrugsbekämpfern darstellen.

Als unsere Branche besser im Aufspüren von Betrug mit Rechenzentren-Bots wurde, spooften die Betrüger die IP-Adressen ihrer Rechenzentren, um sich als Abonnenten großer Internet-Anbieter für Privathaushalte auszugeben. Werbetechnologie wird früher oder später effektive Taktiken für die Betrugsbekämpfung im Zusammenhang mit viralen Inhalten entwickeln und die Betrüger somit in andere Bereiche der Internetwirtschaft verdrängen. Branchenweite Anstrengungen wie die Trustworthy Accountability Group des IAB und ads.txt veranschaulichen bereits heute unsere Entschlossenheit, gemeinsam auf die Eliminierung zwielichtiger Publisher aus der Versorgungskette hinzuarbeiten.

Doch für den Moment müssen Werbetreibende und Publisher mit der Entwicklung einer Roadmap für die Auswertung von viralem Traffic beginnen. Neben dem Identifizieren offenkundig betrügerischer Aktivitäten müssen Branchenakteure sich darüber klar werden, wie sie mit den Grauzonen des Betrugs mit viralen Inhalten umgehen wollen. Was passiert, wenn virale Inhalte eine Mischung aus menschlichem und nicht-menschlichem Traffic anziehen? Was passiert, wenn eine Zielgruppe, die ausschließlich aus echten Menschen besteht, sich auf minderwertige Fake News“-Inhalte stürzt? Die Beantwortung dieser Fragen wird einen wertvollen ersten Schritt im Rahmen unserer Bemühungen zur Lösung dieses Problems darstellen.

Hier bei AppNexus gehen wir das Problem aus mehreren Perspektiven an und setzen dabei auf mehrgleisige Strategien – manche sogar aus den Bereichen Schädlingsbekämpfung und Epidemiologie –, um Betrug zu eliminieren, wo immer wir nur können. Wir nehmen nicht nur Kundenfeedback überaus ernst, sondern investieren außerdem in noch gründlichere Inhaltsanalyse, um die Qualität einer bestimmten Website zu bestimmen. Dazu gehört die Überprüfung von Seiteninhalten, um eventuelle Plagiate aufzudecken und zu beurteilen, ob der Textinhalt eines Beitrags mit dessen URL übereinstimmt.

In der Zwischenzeit möchten wir Ihnen noch eine Reihe hilfreicher Schritte an die Hand geben, die Internetnutzer, Publisher und Werbetreibende schon heute befolgen können, um zur Betrugsbekämpfung im Bereich viraler Inhalte beizutragen.

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

Publisher

- **Lassen Sie beim Erwerb von Traffic größte Vorsicht walten.** Sie sollten jeden Traffic-Anbieter, mit dem Sie zusammenarbeiten, einer genauen Überprüfung unterziehen und bedenken, dass die Wahrscheinlichkeit von Betrug umso höher ist, desto günstiger die Klicks sind – wenn man Ihnen ein Angebot macht, das zu gut klingt, um wahr zu sein, dann ist es das wahrscheinlich auch nicht. Wenn Sie nicht vorsichtig sind, könnten Sie Ihre Reputation auf dem Markt schädigen. Eine gute Frage, die Sie sich stellen sollten, ist, ob dieser Partner über ein Team verfügt, das eigens für Betrug zuständig ist. Das wäre ein gutes Indiz dafür, dass er dieses Problem ernst nimmt und nicht mit gefälschten Benutzern handelt. Eine niedrigere Messlatte für Anbieter besteht darin, die Website des Unternehmens zu überprüfen, um sich zu vergewissern, dass diese für einen seriösen Anbieter angemessen ist. Viele Traffic-Akquise-Unternehmen, die mit betrügerischem Traffic handeln, haben Websites, die lediglich generischen Text und keinerlei Informationen über Mitarbeiter enthalten, was darauf schließen lässt, dass bei dem fraglichen Unternehmen womöglich nicht alles mit rechten Dingen zugeht.

- **Bauen Sie ein engagiertes, treues Publikum auf.** Es ist wichtiger, einen stetigen, dauerhaften Besucherstrom aufzubauen, als sich mit Clickbait und kurzlebiger Aufmerksamkeit zufriedenzugeben. Letzten Endes ist ein ausschließlich viraler Ansatz nicht nachhaltig, da Sie auf ewig von den Algorithmen sozialer Medien abhängig sind.

- **Falls Sie mit betrügerischem Traffic handeln, sollten Sie wissen, dass Ihre Tage gezählt sind.** Mehr und mehr Akteure im Bereich der Werbetechnologie arbeiten an Methoden zur Priorisierung hochwertiger Inhalte. Für Plagiatoren und virale Manipulatoren tickt die Uhr.

Werbetreibende

- **Analysieren Sie Ihre Daten.** Die beste Waffe im Kampf gegen Werbebetrug ist eine Überprüfung Ihrer Versorgungskette mit allen Mitteln, die Ihnen zur Verfügung stehen. Als JPMorgan sich die Zeit nahm, die Websites, auf denen die Anzeigen des Unternehmens platziert waren, manuell zu überprüfen, eliminierte das Unternehmen alle bis auf 5.000 der 400.000 Publisher, mit denen es zusammengearbeitet hatte.

  Bemerkenswerterweise hatten diese Websites keinerlei Auswirkung auf die Performance, was bedeutete, dass das Unternehmen zuvor Anzeigen von 395.000 Publishern gekauft hatte, die nicht den geringsten Mehrwert lieferten.

- **Fragen Sie Publisher, woher ihr Traffic kommt.** Wenn ein Publisher Traffic aus Drittanbieter-Quellen bezieht, sollten Sie den Erwerb dieser Impressions meiden.

 ©2017 AppNexus Inc. Alle Rechte vorbehalten.

- **Sprechen Sie mit Ihren Anbietern und programmatischen Partnern.** Wir bei AppNexus lesen jeden einzelnen Fall, der uns von unseren Kunden zugetragen wird. Wir sind stets bestrebt, mehr über Werbebetrug zu lernen, und wir helfen jederzeit gerne, falls ein Problem vorliegt. Falls es etwas gibt, womit wir Ihnen behilflich sein können, würden wir uns sehr freuen, von Ihnen zu hören

Internetnutzer

- **Informieren Sie sich in Sachen Medienkompetenz.** Lernen Sie, hochwertige Inhalte von fragwürdigen zu unterscheiden.

  Bevor Sie einen Artikel teilen, sollten Sie sich ein wenig auf der entsprechenden Website umsehen, um sich ein Bild von weiteren Artikeln zu verschaffen, die diese veröffentlicht hat. Gibt es andere Quellen, die die Berichterstattung bestätigen? Hat es den Anschein, als ob Zeit und Aufwand in Qualität investiert wurden? Erkennen Sie bei Ihrer Erkundung der Website einen oder mehrere der billigen Tricks, die wir zuvor aufgelistet haben?

- **Wenn Ihnen etwas auffällt, werden Sie laut.** Zögern Sie nicht, sich bei Publishern zu beschweren, wenn Sie auf Anzeigen, Widgets mit gesponserten Inhalten oder Websites stoßen, die Ihnen ein ungutes Gefühl geben. Legitime Medienunternehmen sollten sehr um eine gute Nutzererfahrung bemüht sein.

HAFTUNGSAUSSCHLUSS

Alle Rechte vorbehalten. Die in diesem Whitepaper dargelegten Informationen werden als verlässlich und mit Stand des Erscheinungsdatums als aktuell erachtet. Die Richtigkeit kann jedoch nicht garantiert werden. In diesem Whitepaper enthaltene Empfehlungen oder vorausblickende Aussagen basieren auf Einschätzungen zukünftiger Ergebnisse zum Zeitpunkt des Erscheinungsdatums und sind naturgemäß ungewiss. Die tatsächlichen Ergebnisse können von denen, wie sie in solchen Empfehlungen und vorausblickenden Einschätzungen dargestellt oder angedeutet sind, abweichen. AppNexus unterliegt keinerlei Verpflichtung, seine hier dargestellten vorausblickenden Aussagen als Ergebnis neuer Informationen oder nachfolgender Ereignisse etc. zu aktualisieren oder zu ändern, und widerspricht einer solchen ausdrücklich.


AppNexus