Adjust GmbH Saarbrücker Straße 38a, 10405 Berlin, Germany
Adjust Inc. 535 Mission Street, San Francisco, CA 94105, United States of America
Phone +49 30 91 46 00 83, Fax +49 30 25 74 96 75 www.adjust.com

Neue Form von Mobile Ad Fraud auf Android entdeckt

"Click Injection Fraud" wird eine zentrale Herausforderung für Mobile Werbetreibende in 2017

Berlin, 19.01.2017 - Adjust, das Mobile Attribution und Analytics-Unternehmen und Marktführer in Betrugsprävention, hat eine neue Form des Mobile Ad Frauds auf Android-Geräten entdeckt: den sogenannten "Click Injection Fraud". Fraud-Entwickler machen sich dabei die "Broadcast Intent" Funktion von Android-Geräten zu Nutze, durch die bereits installierte Apps über neue Downloads und Installationen auf dem Gerät informiert werden.

Die neue Fraud-Methode funktioniert dabei wie folgt: Ein Fraud-Entwickler veröffentlicht eine "betrügerische App", die Werbeeinnahmen für den Entwickler generiert, indem die App vorgibt, auf Werbeaktionen zu reagieren. Eine solche App kann ein Solitaire-Spiel oder eine banale Taschenlampen-App sein. Einmal auf dem Android-Gerät installiert, wird diese App durch "Broadcast Intents" über neue Downloads aus dem Google-Playstore informiert. In der Fraud-App wird ausgelöst nach Empfang des Broadcast Intent ein Werbeklick ausgelöst, der den Download fälschlicherweise auf eine Werbemaßnahme zurückführt. Die Betrüger erhalten so unberechtigterweise eine Auszahlung vom Marketingbudget, die typischerweise zwischen $ 1 und $ 5 liegen kann.

"Da die Ansätze, die wir im vergangenen Jahr zur Bekämpfung von Mobile Fraud gestartet haben, sich mittlerweile weit verbreitet haben, sinken die Einnahmen von Fraud-Entwicklern zunehmend. Deshalb finden wir immer wieder neue Formen von Mobile Ad Fraud, die unsere Fraud Prevention Tools umgehen. Es bleibt ein Katz-und-Maus-Spiel", sagt Andreas Naumann, Fraud Prevention Specialist bei Adjust. "Das neue Schema ist technisch ähnlich wie die 'Click-Spamming-Methode', die wir Anfang des vergangenen Jahres bereits beschrieben haben. Sie weicht jedoch den bestehenden Tools aus, die den Klick-Spam verhindern."

Adjust testet derzeit verschiedene Algorithmen, die den Click-Injection Fraud erkennen und betrügerisch generierten Attributions verhindern sollen. Sobald die Algorithmen marktreif sind, werden sie in die Fraud Prevention Suite um die Marketingbudgets zu schützen.

Paul Müller, Co-Founder und CTO bei Adjust, erklärt hierzu: "Fraud Prevention ist ein komplexes Thema, das man mit Vorsicht behandeln muss, da die Änderungen in Echtzeit vorgenommen werden und sich auf die Daten der Analyse auswirken. Jeder überstürzte Versuch, die Daten zu säubern, kann dazu führen, dass Datensätze verfälscht werden. Das ist letztlich das langfristige Problem für datengetriebene mobile Werbetreibende: unsaubere Angaben zu Conversions und verschmutzte Daten."

Fake Conversions schlagen sich nicht nur negativ auf das Werbebudget nieder. Schlimmer noch, sie täuschen Marketingverantwortlichen vor dass manche bezahlte Kampagnen für Nutzer-Akquise besser funktionieren, als sie es eigentlich tun. Es besteht die Gefahr, dass die Vermarkter falsche Entscheidungen treffen, die auf systematischen Ungenauigkeiten basieren. Dies kann bedeuten, dass Werbetreibende weiterhin in Werbung investieren, die relativ ineffektiv ist und potenziell Geld von besser positionierten und besser gestalteten Kampagnen abziehen.

Über Adjust
Adjust (www.adjust.com) ist eines der weltweit führenden Mobile Attribution und Analytics Unternehmen, und offizieller Facebook und Twitter Marketing Partner. Zu den internationalen Kunden von Adjust gehören Rovio – die Entwickler von Angry Birds –, Zalando und Microsoft. Gleichzeitig arbeitet Adjust mit über 120 Rocket Internet Startups zusammen. Target Partners, Capnamic Ventures, Iris Capital, Active Venture Partners und Highland Capital Europe haben bereits in Adjust investiert. Das 2012 gegründete Unternehmen unterhält neben dem Hauptsitz in Berlin weitere Büros in San Francisco, New York, London, Paris, Istanbul, Jakarta, Peking, Tokio, Seoul, Shanghai, Singapur, Sao Paulo, und Sydney.

ENDE

Q&As für Presse

Box: Was ist "Broadcasts Intent"?
Jede Android App sendet Statusänderungen an das Gerät, auch für andere Apps. Die Statusübertragungen werden gesendet, wenn Apps heruntergeladen, installiert oder deinstalliert werden. Diese Funktion ist praktisch, um eine enge Verbindung zwischen verschiedenen Apps herzustellen. Zum Beispiel optimieren die Apps so die Anmeldung mit einem "Deep Link" zu einem kürzlich installierten Passwort-Manager, oder geben den Benutzern direktere Optionen zum Übertragen in einen bestimmten Webbrowser und so weiter.

Ein Beispiel:
John hat eine betrügerische App auf seinem Gerät installiert - in der Regel eine einfache, kostenlose App mit einigen Anzeigen, wie ein Solitaire-Spiel oder eine "Taschenlampe".

Wenn John eine neue App auf sein Gerät herunterlädt, wird jede andere App, die er bereits hat, über die Installation via Android "install broadcasts" informiert.

Die betrügerische App erkennt den Download. Wenn die neue App mit Display-Werbung beworben wurde, gibt es eine Chance, dass die betrügerische App an der Kampagne teilgenommen hat - und so Zugriff auf die Tracking-Codes hat. Mit den Tracking-Codes meldet die betrügerische App den Anzeigen-Netzwerken und Tracking-Services einen Klick von John.
Wenn John dann die neue App zum ersten Mal öffnet, werden verschiedene Analytics-Services informiert und beginnen mit Querverweisen von Klicks von früher zu arbeiten. Dies kann eine lange Zeit nach dem Download sein!

Der legitim aussehende Klick stimmt mit der Geräte-ID von John überein, und seine Installation wird dem betrügerischen Entwickler zugeschrieben - so erhält der Betrüger eine Auszahlung, die typischerweise zwischen $ 1 und $ 5 liegen kann. Wenn der Werbetreibende die Leistung seiner Werbekampagnen überprüft, scheinen mehr Installationen durch Werbung als durch organische Aktivität erzeugt worden zu sein.

Was bedeutet das für Vermarkter?
Fake Admedia Engagement, der die User Interaktion mit dem Werbemittel fälscht, schlägt sich nicht nur negative auf das Werbebudget nieder. Schlimmer noch, Conversions-Daten die durch Fraud verfälscht wurden führen dazu, dass Marketing-Anbietern glauben, dass manche bezahlte Kampagnen für Nutzer-Akquise besser funktionieren, als sie es eigentlich tun.

Die Daten werden verfälscht: Es besteht die Gefahr, dass die Vermarkter falsche Entscheidungen treffen, die auf systematischen Ungenauigkeiten basieren. Dies kann bedeuten, dass Werbetreibende weiterhin in Werbung investieren, die relativ ineffektiv ist und potenziell Geld von besser positionierten und besser gestalteten Kampagnen umleiten.

Für John bedeutet das, dass er weiterhin Anzeigen bekommt, die ihn nicht interessieren.