Pressemeldung

1,1-1,3 Milliarden USD Schaden durch Zurücksetzen von Device IDs – AppsFlyer launcht Echtzeitschutz Protect360

- Schaden durch Zurücksetzen von Device IDs erstmals von AppsFlyer quantifiziert: 50 Millionen USD allein in Deutschland, weltweit über eine Milliarde jährlich
- Anteil dieser Spielart an Download-Fraud doppelt so hoch wie ursprünglich angenommen – jeder zehnte werbeinitiierte App-Download ist Fraud
- AppsFlyer bietet mit Protect360 eine Lösung, die diese Fraud-Art in nahezu Echtzeit bekämpft auf Basis der riesigen Datengrundlage des Analytics-Anbieters und Machine Learning

Berlin, 20.09.2017 – Durch das Zurücksetzen von Device IDs, einer relativ neuen Spielart von Mobile Fraud, ist mobilen Werbetreibenden weltweit jährlich ein Schaden zwischen 1,1-1,3 Milliarden USD entstanden. Allein deutsche Werbekunden haben schätzungsweise 40 bis 50 Millionen USD eingebüßt und sind damit weltweit auf Platz 6 der am stärksten betroffenen Länder. Das Phänomen ist schon länger bekannt. AppsFlyer, die mit 60 Prozent Marktanteil weltweit führende Plattform für die Attribution mobiler Werbung und Marketing-Analytics, hat den Schaden nun erstmals quantifiziert: Der Anteil dieser Betrugsmasche an Download-Fraud ist doppelt so hoch wie ursprünglich angenommen, und jeder zehnte werbeinitiierte App-Download entpuppt sich als Fälschung. 16 der 100 führenden Werbenetzwerke fallen negativ auf, indem über 20 Prozent der von ihnen gelieferten App-Downloads auf das Zurücksetzen von Device-IDs zurückgehen. Diese Erkenntnisse gewann AppsFlyer in den Beta-Tests seiner neuen Anti-Fraud-Lösung Protect360, die ganzheitlich vor Betrug bei App-Downloads schützt und nun für alle Werbetreibenden erhältlich ist.

Der weltweite Markt für mobile Werbung floriert mit einem Gesamtvolumen von 99,3 Milliarden USD laut Prognosen von ZenithOptimedia und zieht als Wachstumsmarkt Betrüger an wie Honig die Bienen. Eine zentrale Rolle spielen Device-Farmen, die auf Tausende mobile Geräte zurückgreifen, um mit gefälschten Klicks, Downloads und Interaktionen einen Teil des Werbebudgets abzuzweigen. Die Verschleierung von Betrug in dieser Größenordnung ist nicht einfach, doch Device-Farmen verbergen ihre Aktivitäten unter anderem, indem sie die IDs jedes einzelnen mobilen Gerätes kontinuierlich zurücksetzen. Dadurch wird jedes verwendete Telefon auch nach Tausenden von wiederholten App-Downloads immer wieder als „neu“ erkannt, wodurch ein jährlicher wirtschaftlicher Schaden in Milliardenhöhe entstand.

Wirtschaftliche Auswirkungen für Deutschland:

- Deutschland ist weltweit auf Platz 4 der am stärksten durch Device ID Reset Fraud betroffenen Länder (gemessen an der Anzahl der gefälschten Downloads) und Platz 6 im Hinblick auf den entstandenen wirtschaftlichen Schaden.
- Allein im Jahr 2017 verloren deutsche Werbekunden zwischen 40 und 50 Millionen Euro durch diese Betrugsmasche.
- Deutschland ist Zielland Nummer 1 beim Device ID Reset Fraud unter iOS (USA auf Platz 4), unter Android liegt Deutschland auf Platz 4.

„Unsere Technologie ist auf 98 Prozent aller Smartphones weltweit zu finden. Aufgrund dieser Datengrundlage und unserer Position im Markt sind wir überhaupt in der Lage, Betrug durch das Zurücksetzen von Device IDs aufzudecken. Würden wir nicht vier Milliarden Geräte bereits kennen, könnten wir Anomalien durch neue Geräte nicht zuverlässig aufdecken“, erklärt Ben Jeger, Managing Director DACH von AppsFlyer. „Protect360 ist ein Wendepunkt und ermöglicht als aktiver Schutz, dass wir zusammen mit den integrierten Werbenetzwerke unsere Kunden noch besser vor Betrug schützen, indem wir mit intelligenten Lösungen auf unserer DeviceRank Datenbank aufbauen.“

Wie Protect360 funktioniert

Protect360 verwendet mehrere Schichten von Anti-Fraud-Technologien für einen nahezu Echtzeitschutz, der betrügerische Downloads blockiert und verdächtige Verhaltensweisen und

anomale Aktivitäten meldet und verhindert. Die Lösung verhindert nicht nur DeviceID Reset Fraud auf SiteID-Ebene und identifiziert betrügerische Geräte, sondern schützt Werbetreibende auch vor anderen Arten von App-Download-Betrug. Dazu gehören unter anderem Hijacking, Click Flooding und Man-in-the-Middle-Attacken. Echtzeitbenachrichtigungen halten die Netzwerkpartner auf dem Laufenden und reduzieren Verhandlungen zwischen Werbekunden und Publishern, die gleichzeitig Betrugsfälle in ihrem Bestand bereinigen können. Durch detaillierte Berichte wissen Marketingverantwortliche, wann und wo Betrugsfälle blockiert wurden, sodass sie mit ihren Netzwerkpartnern proaktive Schutzmaßnahmen ergreifen können.

Zusätzlich zum automatisierten Schutz integriert Protect360 auch AppsFlyers Live Alerts, Validierungsregeln und den IO Builder Fraud Appendix.

- **Live Alerts** benachrichtigen Teammitglieder über Veränderungen ihrer wichtigsten KPIs, einschließlich Betrugs- und Leistungskennzahlen.
- **Validierungsregeln** legen fest, welche Downloads einer Kampagne zugeschrieben werden und welche nicht basierend auf einer Reihe von Kriterien einschließlich Betrugsindikatoren.
- **IO Builder Fraud Appendix** unterstützt Werbetreibende und Netzwerke dabei, langwierige Verhandlungen zu vermeiden, indem Fraud Benchmarks als Teil des IO-Prozesses definiert werden – bereits bevor Anzeigenkampagnen beginnen.

Der vollständige Mobile Fraud Report kann hier heruntergeladen werden:
https://www.appsflyer.com/resources/deviceid-reset-fraud-data-study

Über AppsFlyer
Auf 98 Prozent aller Smartphones weltweit ist die Technologie von AppsFlyer, der führenden Plattform für die Attribution mobiler Werbung und Marketing-Analytics, zu finden. Datengetriebene Vermarkter unterstützt AppsFlyer als unabhängiger Partner für Werbemessung und innovativer Technologieanbieter beim Ausbau ihres Mobilgeschäfts. AppsFlyer trackt jeden Tag Milliarden mobiler Benutzeraktionen und ermöglicht es Werbetreibenden und Entwicklern damit, den Return of Investment ihrer Werbeausgaben zu maximieren. Mit der Attributionslösung NativeTrack™, umfassenden Marketinganalysedaten, dem intelligenten Deeplink namens „OneLink" und der Active Fraud Suite mit dem gerätebasierten Schutz DeviceRank finden Advertiser der erfolgreichsten mobilen Apps der Welt alle Instrumente gebündelt, die sie für die Optimierung ihrer Werbeinvestitionen benötigen. Mehr als 10.000 weltweit führende Marken und Partner, darunter Facebook, Google, Twitter, Pinterest, Tencent, HBO, Playtika, Waze, Alibaba und Kayak, vertrauen auf die Technologie von AppsFlyer. App-Vermarkter können sich an lokale Experten in 12 Standorten weltweit wenden, darunter die DACH-Zentrale in Berlin unter Leitung von Managing Director Ben Jeger.

Weitere Informationen finden Sie unter www.appsflyer.com

Pressekontakt:
Agentur Frische Fische
Gesine Märten
Tel: +49 (0) 351 5635 5661
E-Mail: gm@frische-fische.com