FRAUD TÜRLERİ

iab turkey

FRAUD TÜRLERİ

İnsan Dışı Trafik Kaynakları

Tanım	Açıklama	
1. Cihaz korsanlığı	Kullanıcı kontrolü/rızası dışında kullandığı cihazdan reklam çağrısı yapılması	Fraud
2. Kullanıcı gibi davranan botlar	Kullanıcı gibi mecraları ziyaret eden, sayfaları ziyaret eden tüm bot türleri	Fraud
3. Server kaynaklı trafik	Tek IP'den bağlanan kurumlarda rastlanır. Trafik kullanıcı bilgisayarlarından kaynaklandığında geçerliyken kullanıcı kaynaklı olmayıp, kurumun data merkezi/server kaynaklı trafikler insan dışı trafiktir.	Potansiyel Fraud

FRAUD TÜRLERİ

Diğer Anormal Trafik Kaynakları

Tanım	Açıklama	
4. AdWare trafiği	Belirli yazılımlarla birlikte kullanıcı cihazına yüklenen, kendi başına reklam gösteren ve izinsiz reklam verisi toplayan yazılımların (AdWare) yarattığı reklam trafiği	Fraud
5. Proxy trafik	Kullanıcı trafiğinin proxy cihazlar veya ağlar üzerinden yönlendirildiği durumlar. Bu uygulamada trafik kullanıcı tarafından yaratılır ama kullanıcıya ait bilgi anonimleştirilebilir. Proxy kullanan cihazlardaki trafik kullanıcıya ulaşsa da kaynağı belli değildir. Türkiye'de görünen bir kullanıcı aslında başka bir ülkede olabilir. Bu sebeple reklam hedeflenen kitle dışında birine gösterilebilir.	Fraud
6. Tarayıcı kaynaklı olmayan User Agent başlığı	Bazı cihazlar ve uygulamalar kullanıcı kaynaklı olmayan şekilde ve tarayıcı kullanmadan (Non-browser) mecralara erişim sağlayabilir. Bunlar yayıncının veya başka bir yayıncının app'leri gibi kontrollü erişim olabilir veya crawler'lar gibi kontrolsüz erişim olabilir. Bu erişimler her bir tarayıcının tanım bilgisi (User Agent) içerisinden ayıklanabilir.	Potansiyel Fraud
7. Sayfanın yüklenmesi öncesi reklam çağrılması	Sayfa yükleme aşaması tamamlanmadan (prerender) reklam çağrısı yapılması Mecralar bu işlemi sayfanın hızlı yüklenmesi ve kullanıcı deneyimini artırmak için kullanmaktadır. Fakat hata eseri veya kötü amaçla reklamın önceden yüklendiği sayfada gösterilmemesi veya sayfanın kullanıcı cihazında açılmaması gibi geçersiz sayılması gereken durumlar oluşabilir.	Potansiyel Fraud

FRAUD TÜRLERİ

Kod Korsanlığı

Tanım	Açıklama	
8. Reklam kodu korsanlığı	Bir siteden reklam kodlarının izinsizce alınıp başka bir siteye yerleştirilmesi	Fraud
9. Kreatif korsanlığı	Kreatiflerin marka veya legal hizmet sağlayıcısının izni olmadan kopyalanıp ayrıca yayınlanması	Fraud

FRAUD TÜRLERİ

Site/Gösterim Özellikleri

Tanım	Açıklama	
10. Reklamın otomatik yenilenmesi	Sayfa sabitken reklamın belirli veya rastgele sürelerle otomatik olarak yeniden yüklenmesi Genelde bu durum fraud potansiyeli taşımakla birlikte fraud olmayan uygulamalar da mevcuttur. Örneğin, televizyon kanallarının online mecralarında canlı yayın sayfaları uzun süre açık kalır (Örn. 1 saat). Bu sayfalardaki reklam modelleri reklamverenlerin bilgisi dahilinde belirli sürelerde dönüşümlü satılabilir.	Potansiyel Fraud
11. Reklam yoğunluğu	Sayfadaki/uygulamadaki reklam yoğunluğu Reklam sayısı veya reklam alanı sayfanın toplam alanına oranıyla ölçülür. Reklamverene reklam sayısı/oranı taahhüt edilerek yapılan satışlarda, oranın/sayının taahhüt edilenin üzerinde olması fraud sayılır.	Potansiyel Fraud
12. Gizli reklamlar	Kullanıcıya görünmeyecek şekilde yerleştirilen reklamlar Örneğin, üst üste yüklenmiş reklamlar, %100 saydam yüklenmiş reklamlar vb.	Fraud
13. Çalıntı içerik	Telif hakkı bulunmayan içeriğin yayınlanması	Potansiyel Fraud
14. Kategori sahteciliği	Site içeriğinin olduğundan farklı gösterildiği durumlar Örnek: Spor kategorisinde görünen bir sitenin müzik sitesi olması	Fraud
15. Malware içerme	Kullanıcının bulunduğu sitenin/uygulamanın cihaza yüklemek için kötü amaçlı yazılımlar (malware) bulundurması	Fraud

FRAUD TÜRLERİ

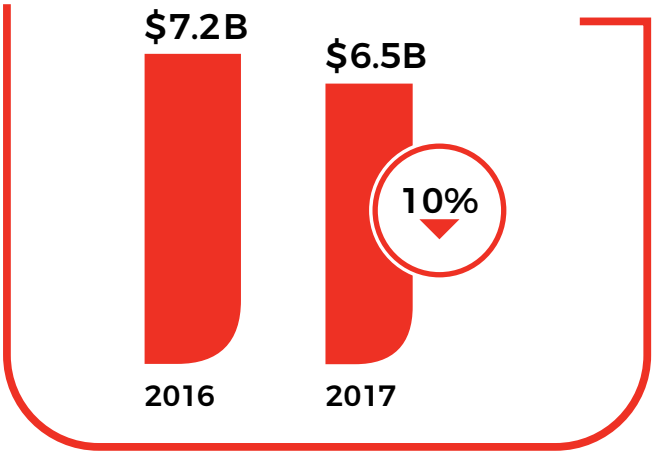
Kreatif/Diğer

Tanım	Açıklama	
16. Cookie sahteciliği	Girilen siteden kullanıcıya sanki diğer sitelere girmiş gibi o sitelerin cookie'lerinin gönderilmesi	Fraud

FRAUD TÜRLERİ

DÜNYADA DİJİTAL REKLAM SAHTECİLİĞİNİN BÜYÜKLÜĞÜ

Danışmanlık firması Price Waterhouse Coopers'ın 'Global Entertainment and Media Outlook 2016-2020' raporuna göre tüm dünyada dijital reklam sahteciliğinin sebep olduğu ekonomik zararın %10'luk gerilemeyle 2017'de 7.2 Milyar $'dan 6.5 Milyar $'a inmesi ön görülüyor. Bu gerilemeye sektörün sahteciliğe karşı önlem almaya başlaması sebep olacak.



ADS.TXT (AUTHORIZED DIGITAL SELLERS) GİRİŞİMİ

Gerekçe: Mevcut durumda IAB'nin OpenRTB Protokolü çerçevesinde satın alınan her impression'un URL adresi ve yayıncı ID'si belirlenebiliyor. Fakat bu envanteri kimin sattığı, bu envanterin yetkili bir satıcının elinden mi, yoksa farklı yöntemlerle izinsiz olarak mı exchangelere sunulduğu belirlenemiyor. Bu da bot trafiği, izinsizce bir envanterin ismini kullanarak başka envanterler satılması, markaların kara listelerinin atlatılması gibi sahtecilik faaliyetlerine kapı aralıyor.

Amacı:

- Programatik reklamcılık ekosisteminde şeffaflığı artırmak
- Mecraların kendi reklam alanlarını satmaya yetkili kuruluşları programatik ekosistemde duyurmasını sağlayarak sahteciliği önlenmek IAB Tech Lab bu amaçla 27 Haziran 2017'de ads.txt çözümünü ve kılavuzunu yayınladı.

ADS.TXT (AUTHORIZED DIGITAL SELLERS) GİRİŞİMİ (Devamı)

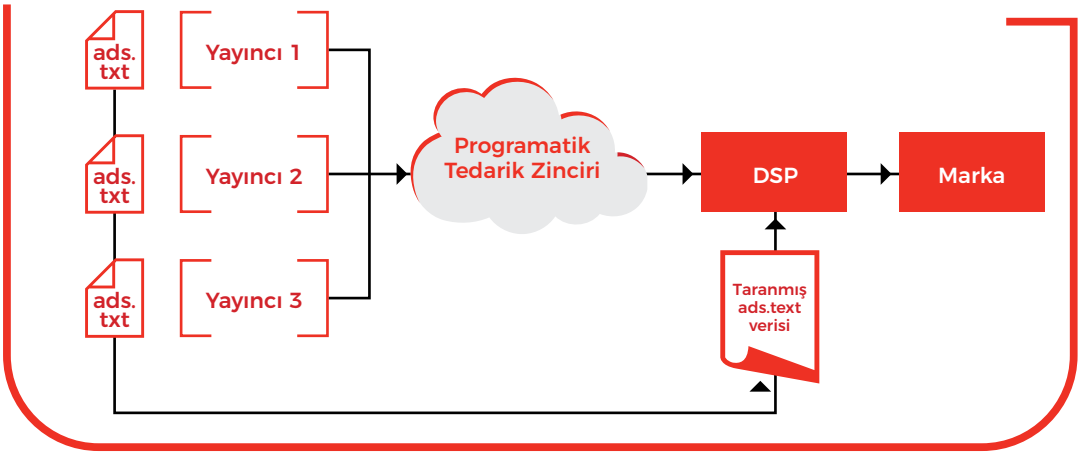
Metodoloji:

- Mecranın webmasteri tarafından sitenin domain üzerinden post edilen bir .txt dosyası. Bu dosya mecranın yetkili satıcılarının listesini içeriyor ve medya satın alması yapacak herkesin ulaşabilmesi için paylaşılıyor.
- Programatik satın alma yapan teknolojiler siteleri tarayarak bu veriye ulaşıyor ve bu sistemdeki tüm yayıncıların yetkili satıcılarını listeliyor. Bu sayede OpenRTB üzerinde teklif vereceği sırada aldığı envanter verisini bu listeye göre filtreleyebiliyor.

Örnek ADS.txt listesi: Example.com sitesi sunucu tarafında aşağıdaki listeyle yetkili satıcılarını account ID'leriyle beraber yayınlıyor:

http://example.com/ads.txt:
#< SSP/Exchange Domain >, < SellerAccountID >, < PaymentsType >, < TAGID >
greenadexchange.com, 12345, DIRECT, AEC242
blueadexchange.com, 4536, DIRECT
silverssp.com, 9675, RESELLER

Artık satın alacak taraf kendini example.com olarak tanıtan bir bid request aldığında requestin sitenin ads.txt dosyasında kayıtlı exchange, SSP ve diğer satıcılardan birinden gelip gelmediğini kontrol edebiliyor.



Kaynak:
Ad Fraud sınıflandırması: http://www.jicwebs.org/images/JICWEBS_Traffic_Taxonomy_October_2015.pdf
Ads.txt ana sayfası: https://iabtechlab.com/ads-txt/
Ads.txt kılavuzu: https://iabtechlab.com/wp-content/uploads/2016/07/IABOpenRTBAds.txtSpecification_Version1_Final.pdf