White Ops


L’attaque de bot
la plus importante
de la télévision
connectée

White Ops

# L'attaque de bot la plus importante de la télévision connectée

Chercheurs : Dr. Mike Moran, Mikhail Venkov, Ryan Castellucci, Aaron DeVera, et Davide Mandrini

La télévision connectée (CTV) offre d'immenses possibilités de diffusion en continu de services et de marques qui permettent d'entrer en contact avec les consommateurs par le biais de publicités et de contenus attrayants. En raison de cette opportunité, il est incroyablement important pour l'écosystème et les opérateurs de CTV de travailler ensemble sur une chaîne d'approvisionnement publicitaire protégée collectivement, afin de s'assurer que la fraude soit decouverte, traitée et éliminée le plus rapidement possible, car les mauvais acteurs suivent toujours l'argent. La fraude publicitaire peut se produire lorsque vous achetez des inventaires par le biais de canaux non protégés. Elle peut être éliminée rapidement par des canaux protégés où il existe des relations directes, de la confiance et une transparence totale. La collaboration au sein d'une chaîne d'approvisionnement collectivement protégée permet à l'écosystème de tirer pleinement

parti des avantages de la création d'une expérience exceptionnelle pour le client sur la CTV, exempte de fraude publicitaire.

Une nouvelle opération de fraude publicitaire sur la CTV, baptisée ICEBUCKET, a été lancée dans une partie de la publicité programmatique où la chaîne d'approvisionnement est moins transparente, où les vendeurs ne sont pas signalés dans les fichiers sellers.json et où les acheteurs et les vendeurs n'ont généralement pas de relation directe. Les acteurs frauduleux à l'origine d'ICEBUCKET ont eu de bons résultats jusqu'à ce qu'ils essaient d'étendre et d'intensifier leurs efforts. Cependant, en travaillant avec nos partenaires, nous avons bloqué l'attaque, protégé et partagé les données à travers notre réseau, et amélioré l'efficacité de notre plateforme pour nous assurer que nous restons en avance sur la fraude publicitaire et les criminels qui l'exploitent. Notre succès est lié à une planification à long terme ainsi qu'aux processus et aux pratiques en place entre nous et nos partenaires.

L'équipe Satori de White Ops pour la recherche et le renseignement sur les menaces a récemment découvert la plus grande et la plus vaste opération de fraude liée à la télévision connectée (CTV) à ce jour. À son apogée, l'opération du bot ICEBUCKET s'est fait passer pour plus de 2 millions de personnes dans plus de 30 pays. L'opération a contrefait plus de 300 éditeurs différents, volant les dépenses publicitaires en faisant

croire aux annonceurs qu'il y avait de vraies personnes de l'autre côté de l'écran, alors qu'en réalité, il s'agissait de bots prétendant être de vraies personnes regardant la télévision. L'opération a dissimulé ses bots sophistiqués grâce aux limites de la transparence et du signal des impressions publicitaires vidéo soutenues par l'insertion de publicités côté serveur (SSAI). La plateforme de lutte contre les bots de White Ops est capable de détecter cette fraude, de protéger ses partenaires contre les risques et de les empêcher d'êtres victimes de cette opération et d'autres du même type.

Voici les détails sur la façon dont l'opération ICEBUCKET a été détectée et comment nous l'avons empêché d'avoir un impact sur une chaîne d'approvisionnement protégée collectivement. Dans un effort pour protéger davantage les annonceurs, nous présentons nos recommandations aux différents opérateurs de la CTV afin de rester à l'abri de la fraude.

## *28% des dépenses gaspillées*

L'opération ICEBUCKET est le plus grand cas d'usurpation d'identité sur la SSAI qui ait été découvert à ce jour. Selon nos données internes, basées sur la visibilité de White Ops, près de 28% des opérations sur la CTV sur environ 1,9 milliard de demandes de publicité par jour pour le mois de janvier, provenaient de cette seule opération.

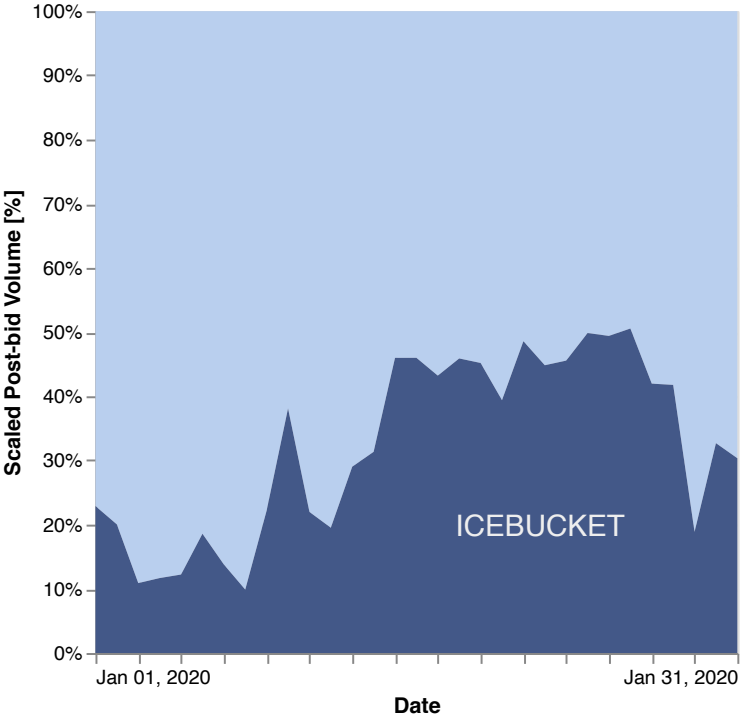


*Figure 1 : pourcentage d'achat programmatique sur la CTV détourné par cette opération pour janvier 2020.*

En janvier 2020, 66 % des achats programmatiques de SSAI liés à la CTV et 15 % du trafic SSAI programmatique lié à la téléphonie mobile, que White Ops protège, faisaient partie de ce graphique. Lorsque nous examinons les appareils utilisés dans le cadre de l'opération, nous voyons différents appareils de CTV à côté du traf-

ic mobile. Les principales plateformes  usurpés dans ce système sont indiqués ci-dessous. Certaines des plateformes que les fraudeurs ont usurpés dans le cadre de cette opération proviennent de lignes de produits discontinuées. White Ops a fourni des informations sur cette menace à Roku, ce qui leur a permis de vérifier les résultats par rapport à leurs systèmes internes. Ils ont confirmé le caractère frauduleux de l'opération, car il n'y avait aucune activité d'ICEBUCKET sur la plateforme même de Roku.

| Appareils | Proportion [%] |
|---|---|
| Roku (tous les modèles) | 46.0% |
| Samsung Tizen Smart TV | 26.8% |
| Google TV | 20.7% |
| Android (mobile) | 6.1% |

*Tableau 1 : Proportion du trafic ICEBUCKET en janvier 2020 pour différentes plateformes déclareés*

Cette opération a masqué les serveurs SSAI en générant du trafic pour des appareils fictifs de pointe (en particulier la CTV et les appareils mobiles) dans l'écosystème des technologies publicitaires. Pour ce faire, l'opération a utilisé :

- Plus de 1 000 agents utilisateurs différents, dont environ 500 n'apparaissent que dans cette

opération

• Plus de 300 appIDs différents de divers éditeurs

• Au moins 2 millions d'adresses IP usurpées provenant de plus de 30 pays, dont plus de 99 % sont situées aux États-Unis

• Environ 1 700 adresses IP de serveurs SSAI situés dans 9 pays générant le trafic

Afin de comprendre pleinement l'ampleur de l'opération ICEBUCKET, il est important de comprendre comment fonctionne la SSAI, le rôle qu'elle joue dans la publicité programmatique sur les plateformes de CTV, pourquoi l'usurpation d'identité de SSAI est si difficile à détecter, et ce qui fait de la SSAI une cible si attrayante pour les fraudeurs.

## *Qu'est-ce que l'insertion de publicité côté serveur (SSAI) ?*

L'insertion de publicité côté serveur, ou SSAI, a été développée par les éditeurs pour créer une meilleure expérience publicitaire pour l'utilisateur final. Les publicités sont « cousues » dans la trame du contenu vidéo afin d'éviter les retards ou les contretemps causés par le lancement d'un serveur publicitaire.

La SSAI est couramment utilisé pour la publicité sur plusieurs types d'appareils « de pointe », tels que les CTV, les smart-phones, les consoles de jeux et autres. La diffusion de contenu publicitaire vidéo par le biais de la SSAI offre aux annonceurs de nombreux avantages, notamment la personnalisation de la publicité pour l'utilisateur et la réduction du temps de latence.

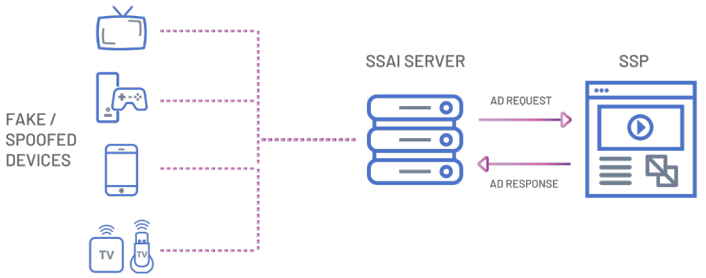


*Figure 2 : Schéma de l'interaction entre les plateformes usurpées et l'écosystème des technologies publicitaires*

Si la SSAI est une solution élégante pour la diffusion de publicités, elle n'en est encore qu'à ses débuts. Comme pour toutes les nouvelles technologies, les fraudeurs parviennent à trouver des failles dans le système et à les exploiter. Les fraudeurs ont ainsi trouvé un moyen d'usurper les périphériques pour l'usurpation de SSAI, la principale technique de fraude utilisée par les opérateurs d'ICEBUCKET, se produit lorsque les fraudeurs envoient un tas de demandes de publicité depuis des centres de données pour des dispositifs « usurpés

» ou de faux périphériques. La source du centre de données est attendue pour les véritables fournisseurs de SSAI. Plutôt que de montrer les publicités aux humains, les fraudeurs lancent les API de signalement indiquant que la publicité a été « visionnée ». Souvent, les informations dont disposent les annonceurs dans un environnement SSAI se limitent à l'agent utilisateur et à l'adresse IP de l'appareil. Ces informations peuvent être envoyées dans les en-têtes HTTP « Appareil-X-Agent-Utilisateur » et « Appareil-X-IP », conformément aux Directives VAST de IAP, ou par d'autres en-têtes similaires. Bien que la falsification de ces données soit relativement simple, la capacité de le faire de manière convaincante démontre le niveau de sophistication de ce bot.

Les annonceurs paient pour que leurs publicités soient visionnées par un public réel ouvert à leurs produits ou services. Au lieu de cela, ces fraudeurs prennent l'argent des annonceurs et l'empochent ; les publicités qui sont « délivrées » ne voient jamais la lumière du jour ou ne sont jamais vues par un être humain. Un public de bots sophistiqués n'est en réalité qu'un public vide.

## *L'opération ICEBUCKET*

L'opération ICEBUCKET a présenté son trafic comme provenant d'un fournisseur SSAI légitime (basé sur l'inclusion d'en-têtes HTTP standard) pour une variété de dispositifs et d'applications, en utilisant un code

personnalisé. ICEBUCKET a rassemblé des demandes d'insertion de publicités dans le contenu vidéo pour les téléspectateurs utilisant des appareils CTV et mobiles, mais aucun de ces appareils ou téléspectateurs n'existe réellement. Les agents utilisateurs utilisés dans le cadre de l'opération se réfèrent en grande partie à des types d'appareils obsolètes qui ne sont plus utilisés dans la population générale, ou à des appareils qui n'ont jamais existé au départ. Les adresses IP ont montré des signes de génération algorithmique pour imiter les audiences souhaitées.

Ces demandes publicitaires provenaient d'un petit ensemble de Numéros de Systèmes Autonomes (ASN). Les systèmes autonomes constituent l'infrastructure de routage d'arrière-plan de l'internet, de la même manière que les routes relient les différentes villes. Chaque système est identifié par un numéro, l'ASN, dont la fonction est similaire à celle d'un code postal. Bien que nous ne puissions pas connaître avec certitude les motivations des acteurs derrière cette menace quant à l'utilisation de ces ASN dans l'opération, nous pouvons faire quelques commentaires sur les raisons possibles. Les ASN ont :

- Une faible application de la part des opérateurs de réseau concernant les activités malveillantes menées à partir de leur centre de données

- Des serveurs privés virtuels (VPS) bons marchés disponibles

- Un grand nombre d'hôtes au sein de cet espace IP qui sont vulnérables ou ouverts à l'exploitation

Il est probable que les acteurs derrière ICEBUCKET aient opéré à partir de ces ASN en raison de la faible possibilité de détection de ces derniers. Tout le trafic provenant de ces ASN ne fait pas partie de l'opération ICEBUCKET, car il y a aussi du trafic régulier provenant de ces ASN.

L'opération ICEBUCKET est unique en ce sens qu'un sous-ensemble du trafic est généré pour bénéficier directement aux éditeurs d'applications par le biais d'accords directs. Nous avons observé des cas où ces éditeurs mélangent le trafic réel et le trafic ICEBUCKET dans ce qui semble être les premiers signes de schémas d'approvisionnement pour le trafic CTV. Notre observation de ce trafic « mélangé » nous a permis de formuler deux hypothèses sur les raisons de ce phénomène :

- **Cacher l'opération :** En créant un sous-ensemble de trafic qui ne bénéficie pas directement à l'opération, les fraudeurs ont créé du « bruit » autour de l'identification de l'opération. Les applications usurpées sont alors

des bénéficiaires involontaires du trafic généré.

• **Fraude en tant que service :** L'opération génère du trafic pour le compte des éditeurs d'applications. Le sous-ensemble d'activités frauduleuses devient plus difficile à détecter et l'opération constitue une source de revenus supplémentaire pour le système.

À ce stade, nous ne pouvons pas faire de distinction définitive entre ces deux possibilités. Il est possible que ces deux options soient en jeu, selon le sous-ensemble particulier du trafic en question.

## *Geler les fraudeurs*

La plateforme de lutte contre les robots de White Ops nous permet de protéger nos partenaires en arrêtant les bots sophistiqués une fois que nous avons identifié avec précision les signatures de la menace. En surveillant les signatures de ces menaces dans notre trafic en amont, nous pouvons automatiquement bloquer le trafic frauduleux et nous assurer que l'argent ne va pas dans les poches des fraudeurs. La plateforme nous permet également de mettre en évidence les parties de l'écosystème technologique où cette opération est florissante, afin que nos partenaires puissent prendre des mesures appropriées de leur propre chef.

L'usurpation, quelle qu'en soit la forme, vise à faire

ressembler l'entité usurpée à la victime (un consommateur, un annonceur, un développeur d'applications - la cible dépend de l'opération). En utilisant plusieurs marqueurs de fraude, nous pouvons distinguer le trafic réel, le trafic humain et le trafic de ces dispositifs usurpés. White Ops fait tout pour ne pas nuire aux applications victimes de fraudes, ce n'est pas parce que les fraudeurs profitent de leurs appID qu'elles doivent être pénalisées. Nous nous efforçons de réduire le flux d'argent vers les véritables fraudeurs, et non vers les organisations qu'ils ciblent.

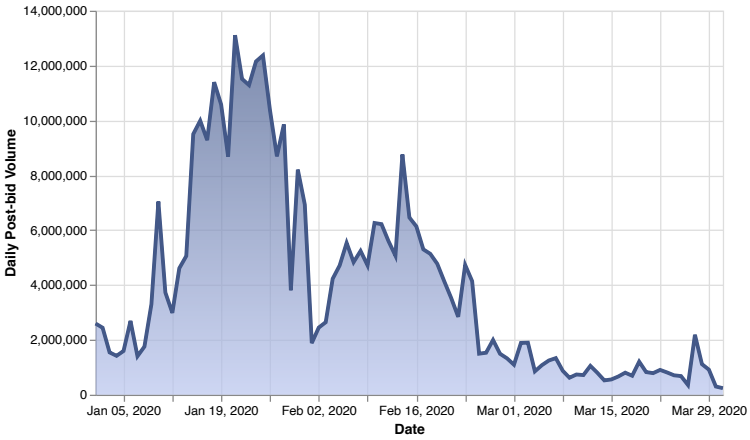


*Figure 3 : impressions post-bid associées à l'ICEBUCKET pour 2020.*

Comme indiqué ci-dessus, l'ICEBUCKET est une opération en cours. Les volumes indiqués dans la figure 3 ne sont pas tombés à zéro. Les fraudeurs sont toujours

dans la nature, mais nous sommes en mesure d'appliquer nos techniques d'atténuation et de prévention envers les bots pour les détecter et protéger contre leurs attaques ; nous divulguons cette découverte maintenant pour que d'autres puissent faire de même. Nous avons déjà déployé des défenses contre des opérations similaires et avons étendu notre couverture de protection collective au sous-ensemble « présumé SSAI » de notre trafic observé. Nos techniques de détection et de prévention des bots évoluent en permanence pour contrer les menaces émergentes, ainsi que pour en anticiper de nouvelles.

## *Stopper la tempête*

Comme l'usurpation d'identité sur la CTV et les SSAI sont actuellement des options lucratives pour nos adversaires en raison des CPM élevés des consommateurs de CTV, nous nous attendons à ce que des opérations similaires commencent, ou que les opérations existantes passent du web et du mobile au trafic de la CTV.

Voici quelques mesures que nos pairs peuvent prendre pour tenter d'atténuer l'usurpation d'identité liée au SSAI :

- Assurez-vous de travailler avec une chaîne d'approvisionnement en publicité protégée collectivement, où il existe des relations

directes, de la confiance et une transparence totale

• Vérifiez la cohérence des déclarations appID/bundleID afin de renforcer les liens entre l'application et l'éditeur, telles que les directives de l'IAB pour l'identification des applications

• Consultez fréquemment vos partenaires publicitaires pour vous assurer que ce nouveau modèle de menace est bien compris par tous ceux qui se trouvent dans votre réseau

• Développez davantage de normes qui augmenteront la transparence de l'inventaire des CTV, par exemple :

  • Étendre la norme app-ads.txt pour prendre en charge le trafic CTV.

  • Adopter pleinement sellers.json pour favoriser la visibilité sur l'ensemble de la chaîne d'approvisionnement.

  • Les fabricants d'appareils et les fournisseurs de SSAI devraient soutenir l'élaboration et l'adoption de normes qui vérifient l'authenticité d'un appareil (par exemple en signant leurs demandes de manière cryptographique). Ce serait

un grand pas en avant dans la lutte contre l'usurpation des dispositifs.

Nous avons vu des actions de ce type avoir un effet positif. Lorsque le dispositif devient moins rentable, alors nous avons fait notre travail : en coupant les sources de revenus des fraudeurs, nous les poussons hors de l'écosystème. Avec l'aide de nos partenaires, White Ops' Advertising Integrity propose une chaîne d'approvisionnement publicitaire protégée collectivement afin de garantir que les annonceurs ne soient pas victimes des attaques de bots les plus sophistiquées sur la CTV et sur Internet.

Le fait d'informer et d'éduquer, sur l'usurpation SSAI, n'est qu'un début - les équipes doivent commencer à surveiller ce comportement. L'écosystème de la publicité programmatique a besoin de normes industrielles afin de « geler » ces fraudeurs une fois pour toutes.

## *Annexe*

Sous-ensemble d'ASN identifiés comme étant les sources de trafic pour cette opération :

| |
|---|
| 29182 |
| 49392 |
| 51167 |
| 51659 |
| 59729 |
| 203004 |
| 204490 |
| 204601 |
| 204957 |

Tout le trafic provenant de ces ASN ne fait pas partie de l'opération ICEBUCKET, car il y a aussi un trafic normal provenant de ces ASN.

Agents-utilisateurs présents : icebucket-uas.txt

> Les agents utilisateurs inclus ne sont pas tous uniques à l'opération ICEBUCKET. Comme l'opération tente de ressembler à un trafic légitime, certains dispositifs représentés ici seront vus en dehors de cette opération.

White Ops®

White Ops is the global leader in bot mitigation. We protect more than 200 enterprises - including the largest internet platforms - from sophisticated bots by verifying the humanity of more than one trillion online interactions every week. The most sophisticated bots look and act like humans when they click on ads, visit websites, fill out forms, take over accounts, and commit payment fraud. We stop them. To learn more, visit whiteops.com.