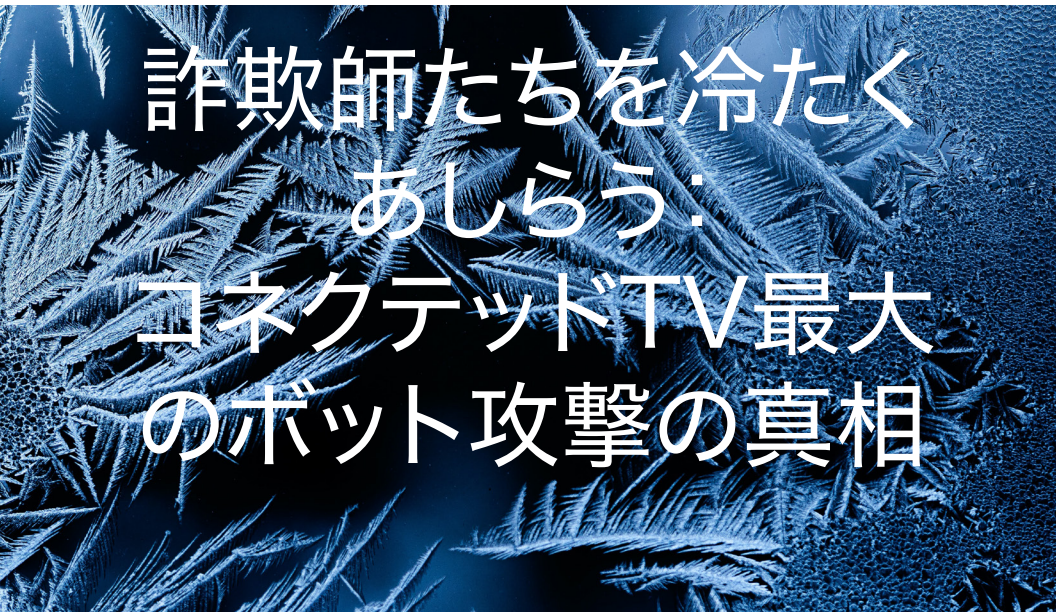
詐欺師たちを冷たく
あしらう：
コネクテッドTV最大
のボット攻撃の真相

White Ops

詐欺師たちを冷たくあしらう：コネクテッドTV最大のボット攻撃の真相

研究員：マイク・モラン博士、ミハイル・ヴェンコフ、ライアン・カステルッチ、アーロン・デヴェラ、ダビデ・マンドリーニ

コネクテッドTV(CTV)は、ストリーミングサービスやブランドにとって、魅力的なコンテンツや広告を通じて、消費者との関わりを持つ、大きな機会を提供しています。そして、このような機会があるため、CTVエコシステムとブランドは、不正行為を共に、認識し、対処し、可能な限り迅速に排除するために、集団的に保護された広告サプライチェーンによって、協力していくことが非常に重要です。広告詐欺は保護されていないチャンネルで在庫を購入した場合に発生する可能性があります。広告詐欺は直接の関係性があり、信頼と透明性のある、保護されたチャンネルを介して迅速に排除することができます。保護されたサプライチェーンを通して協力することで、エコシステムは広告詐欺のない素晴らしいCTVの顧客体験を実現することができることになります。

ICEBUCKETと名付けられた新しいCTVの広告詐欺は、サプライチェーンの透明性が低く、売り手はsersers.jsonファイルで報告されておらず、買い手と売り手は一般

White Ops

的に直接の関係を持っていないプログラマティック広告の一部で始まりました。ICEBUCKETの背後にいる悪質業者は、彼らが拡大を試みるまでは良い方向に進んでいました。しかしながら、私達のパートナーと協力することで、攻撃をブロックし、パートナーネットワーク全体でデータを保護、共有し、プラットフォームの有効性を向上させ、広告詐欺や、その背後にいる悪質業者から、先手を打つことができるようになりました。当社の成功は、当社とパートナーの間で長期的な計画、プロセス、および実践が行われていることを物語っています。

ホワイトオプス・サトリ・スレットインテリジェンスとリサーチチーム(The White Ops Satori Threat Intelligence and Research team)は最近、コネクテッドTV(CTV)関連の詐欺行為の中で最大かつ広範囲に及ぶものを発見しました。ICEBUCKETボット・オペレーションはピーク時には30か国以上で200万人以上になりすましていました。この操作では、300以上の異なるパブリッシャーを偽造し、画面の向こう側に本物の人間がいると思わせることで広告主を騙し、広告費を盗み出しました。このオペレーションはサーバーサイド広告挿入(SSAI)を背景にしたビデオ広告のインプレッションの中に、その洗練されたボットを隠すという仕組みになっています。ホワイトオプスのボット軽減プラットフォームは、この詐欺スキームを検出し、このオペレーションや類似の不正行為の犠牲になることからパートナーを保護することができます。

ここでは、ICEBUCKETオペレーションがどのようにして検出され、集団的に保護されたサプライチェーンに影響を与えないように阻止されたかについての詳細をご紹

介します。広告主の保護を強化するために、CTVエコシステムとブランドが不正行為をしないようにするための推奨事項の紹介です。

ワンアイス、ツーアイス、28%アイス

ICEBUCKETオペレーションは、これまでに発見されたSSAIスプーフィングの最大のケースです。当社の内部データによると、ピーク時にはホワイトオプス社が可視化しているプログラマティックCTVトラフィックの28%近く、つまり1月の1日あたり約19億件の広告リクエストがこの1つのオペレーションから発生していました。

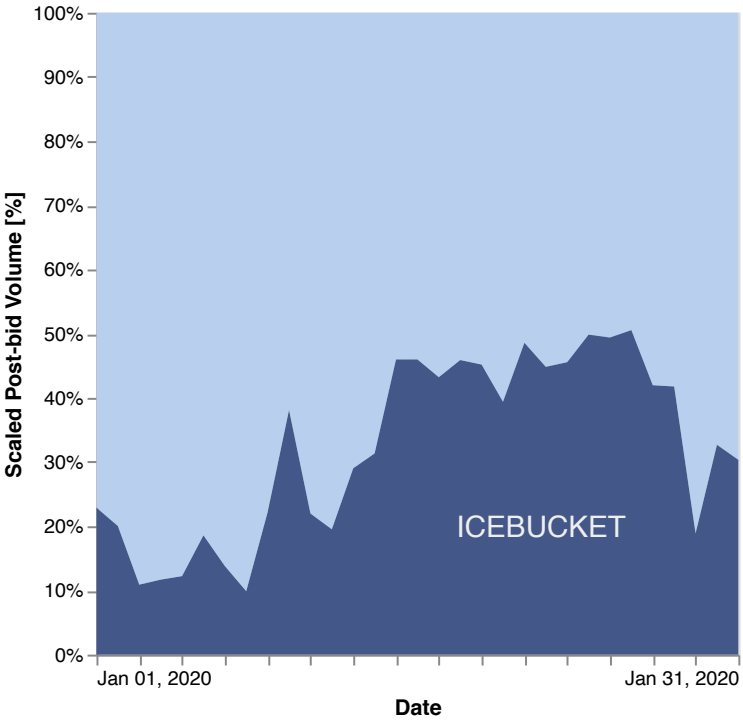

図1：2020年1月のこのオペレーションに関与しているプログラマティックCTVトラフィックの割合

2020年1月には、ホワイトオプス社が保護しているプログラマティックCTV関連のSSAIトラフィックの66%、プログラマティックモバイル関連SSAIトラフィックの15%がこのスキームに含まれた。このオペレーションに使用されたデバイスを見ると、モバイル・トラフィックと並んで様々なCTVデバイスが見られます。このスキームにおける上位のなりすましデバイスを以下に示します。このオペレーショ

ンで詐欺師たちがなりすましたデバイスの中には、製造中止になった製品ラインのものもあります。ホワイトオプス社は、この脅威に関する情報をRoku社に提供し、その結果を社内システムと照合することができ、Roku社はそのプラットフォーム上ではICEBUCKETのオペレーションの活動がなかったことを確認しました。

デバイス	割合[%]
Roku (all makes)	46.0%
Samsung Tizen Smart TV	26.8%
Google TV	20.7%
Android (mobile)	6.1%

表1：2020年1月の様々な公表されたデバイスにおけるICEBUCKETトラフィックの割合

このオペレーションは、架空のエッジデバイス(具体的にはCTVとモバイルデバイス)のトラフィックをアドテックエコシステムに生成することで、SSAIサーバーを偽装しました。
このオペレーションでは

- 1000以上の異なるユーザーエージェントが使用されており、そのうち約500のユーザーエージェントがこのオペレーションでのみ使用されていました。
- 様々なパブリッシャーの300以上の異なるappID

が使用されました

- 30か国以上から少なくとも200万個のIPアドレスを偽装して使用しており、そのうち99%以上がアメリカ国内にあります。
- トラフィックを生成する9か国にある約1700のSSAIサーバーIPを使用しました。

ICEBUCKETのオペレーションの大きさを完全に理解するためには、SSAIがどのように機能するのか、CTVプラットフォーム上のプログラマティック広告で果たす役割、SSAIのなりすましを検出するのが難しい理由、そしてSSAIのなりすましが詐欺師たちにとって魅力的なターゲットになっている理由などを知っておくことが重要です。

サーバーサイド広告挿入(SSAI)とはなにか？

サーバーサイド広告挿入(SSAI)はエンドユーザーの広告体験を向上させるためにパブリッシャーによって開発されました。広告が動画コンテンツに"ステッチング"されているため、広告プレーヤーの起動による遅延などが発生しません。SSAIは一般的に、CTV、スマートフォン、ゲーム機などの"エッジ"デバイスの広告に使用されています。SSAIを利用して動画広告コンテンツを配信することで、ユーザーの個別化や待ち時間の短縮など、広告主に多くのメリットがあります。

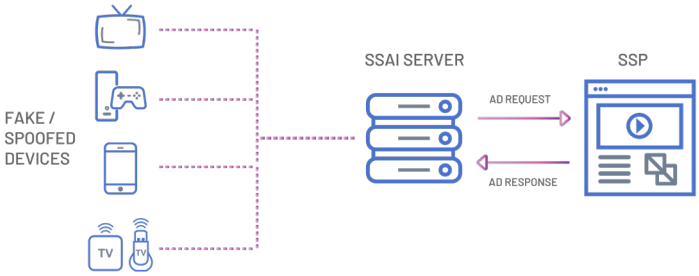

図2：SSAIスプーフィングとアドテックエコシステムとの関係概略図

SSAIは広告配信の素晴らしいソリューションですが、まだ黎明期にあります。ホワイトオプス社は、詐欺師たちがシステムの穴を見つけて、それをすり抜ける方法を見つけることができます。彼らは、SSAIサービスを複製し、エッジデバイスに成りすます方法を見つけたのです。

ICEBUCKETの運営者が使用した重要な詐欺技術であるSSAIなりすましは、詐欺師たちがデータセンターから"なりすまし"または偽装されたエッジデバイスに広告リクエストの束を送信することで発生します。データセンターのソースは、本物のSSAIプロバイダーを想定していますが、詐欺師たちは、人間に広告を見せるのではなく、広告が"表示された"ことを示すレポートAPIを呼び出します。多くの場合、SSAI環境で広告主が利用できる情報はデバイスのユーザーエージェントとIPアドレスに限定されています。この情報は、IAB VAST ガイドラインに従って"X-Device-User-Agent"および"X-Device-IP"HTTPヘッダーで送信されるか、他の類似したヘッダーを介して送信されます。このデータを改ざんするのは比較的簡単で

すが、このニュアンスからすると、これは洗練されたボット攻撃の一形態になります。

広告主は、その製品やサービスを利用している視聴者に表示されるように、広告費を支払っています。しかし、詐欺師たちは、その広告費を自らの懐に入れているというのが現在の状況です。その"提供された"広告は人の目に入ることも、視聴にされることもありません。このような洗練されたボットは、存在しない架空の視聴者と言っても過言ではありません。

ICEBUCKETオペレーション

ICEBUCKETはカスタムコードを使用して、様々なデバイスやアプリ向けに(標準的なHTTPヘッダーを含むことに基づいて)正当なSSAIプロバイダーからのトラフィックを提示していました。ICEBUCKETはCTVやモバイルデバイスを利用している視聴者向けの動画コンテンツに広告を挿入するためにリクエストを組み立てましたが、実際はそれらのデバイスや視聴者は存在していなかったのです。このオペレーションで使用されたユーザーエージェントは、一般の人々が使用していないような時代遅れのデバイスタイプや、そもそも存在しなかったデバイスを主に指しています。このIPアドレスは望ましい視聴者を模倣するためにアルゴリズム的に生成された兆候を示しています。

これらの広告リクエストは、自律システム番号(ANS)の小さなセットから要求されています。自律システムは、道路が異なる都市間のトラフィックを接続するのと

White Ops

同じように、インターネットのバックエンド・ルーティング・ストラクチャーを構成しています。各システムはASNという番号で識別され、郵便番号に似た機能を持っています。不正行為者がこれらのASNをオペレーションに使用する動機は分かりませんが、考えられる理由をいくつか以下に示します。

- ASNはデータセンターから行われる悪意のある活動に関して、ネットワークオペレーターの強制力が弱い。
- ASNは格安のバーチャル・プライベート・サーバ(VPS)サービスが利用可能
- ASNは、そのIP空間内に多数のホストが存在し、脆弱性があるか、もしくは悪用される可能性がある。

ICEBUCKETの背後にいる業者は、自分らの行動は見つからないという確信から、これらのASNからオペレーションしていた可能性が高いです。これらのASNからのトラフィックの全てがICEBUCKETオペレーションの一部というわけではなく、実際にはASNsからのICEBUCKET以外のトラフィックも存在しています。

ICEBUCKETオペレーションは、直接取引を行うことで、アプリパブリッシャーに直接利益をもたらすトラフィックのサブセットが生成されるという点では独特なプログラムです。このようなパブリッシャーがCTVトラフィックのトラフィックソーシングスキームの初期兆候であり、オーガニックトラフィックとICEBUCKETトラフィックが混合しているケースを注意深く監視してみました。この「混合」したトラフィックを観察した上で、これが発生する理由につい

て2つの仮説をまとめました:

- オペレーションの隠蔽:
オペレーションに直接利益をもたらさないトラフィックのサブセットを生みだすことで, 詐欺師達はオペレーションの存在が特定されないことを防ぐノイズを作成しました。スプーフィングされたアプリは、生成されたトラフィックに対して無意識のうちに利益をもたらします。

- サービスとしての不正:
オペレーションはアプリパブリッシャーの代わりにトラフィックを生成します。不正行為のサブセットは検出が困難になり、このオペレーションにはスキームに対しての追加の収入源を生み出します。

現時点では、これら2つの可能性を決定的に判断することはできません。しかし、問題提起されているトラフィックの特定のサブセットによっては、これらの行為の両方が機能している可能性があります。

詐欺師を撃退

ホワイトオプスボットプラットフォームでは、パートナー達を保護するために、特定した脅威となる不正のシグネチャを正確に特定し、高度に設計されたボットを停止します。入ってくるトラフィックを利用し、脅威となる不正のシグネチャを監視することで、不正なトラフィックを自動的にブロックし、詐欺師の懐にお金が入らないようにします。また、このプラットフォーム上では、この様な洗練された操作がアドテックエコシステムに行われるため、パート

ナーは自分の手で行動を起こすことができます。

あらゆる種類のスプーフィングは、スプーフィングされたエンティティ又は組織を被害者（消費者、広告主、アプリ開発者 - ターゲットはオペレーションによって異なる）に似せるように設計されています。
いくつかの詐欺マーカーを使用することで、実際の人のトラフィックとスプーフィングされたデバイスからのトラフィックを区別できるようになります。ホワイトオプスは、詐欺師がappIDを利用しているという理由だけで、詐欺スキームの被害者であるアプリに悪影響を与えないよう考慮された上で設計されています。私たちは、彼らが標的とするエンティティ又は組織ではなく、実際の詐欺師へ流れるお金の流通を削減するために作業取り組んでいます。

図２：2020年のICEBUCKETに関連付けられたビッド後のインプレッション。

上記のように、ICEBUCKETは進行中のオペレーションです。図3に示されている通り、ボリュームはゼロにはなっていません。詐欺師はまだ存在しますが、ボット緩和およびボット防止技術を実行してそれらを検出し、攻撃から保護する作業に励んでいるのが現状です。他の人達がこの情報を参考にして同じことができるように、この発見と研究結果を公開しています。私たちはすでに、同様のオペレーションに対する防御策を展開しており、集団保護の対象範囲を、観測されたトラフィックの「意図されたSSAI」サブセットを元にさらに拡大しています。当社の検出およびボット防止技術は、新しい脅威又は不正を予測するだけでなく、緊急の脅威に対抗できるように継続的に進化しています。

アイス・ストームを止める

CTVとSSAIのスプーフィングは、CTVの消費者のCPMが高く、私たちの敵である詐欺師にとって有利なオプションであるため、同様のオペレーションが開始されるか、既存のオペレーションがWebおよびモバイルからCTVトラフィックにシフトする可能性があると考えられます。

下記の通り、他の同業者達がSSAIのなりすましを緩和するためにできることがいくつかあります。

- 直接的な関係、信頼、完全な透明性のある、集団的に保護された広告サプライチェーンとの連携。
- IABアプリ識別ガイドラインなど、アプリからパブリッシャーへのより強力なリンクを提供するための一貫したappID / bundleIDを使用

White Ops

- エコシステム全体のアドテックパートナーと頻繁に相談し、新しい脅威モデルがステークホルダー全員に十分に理解されていることを確認
- 次のような、CTVインベントリの透明性を高める標準をさらに開発；
  - app-ads.txt 標準を拡張して、CTVトラフィックを完全にサポート
  - サプライチェーン全体の可視性をサポートするsellers.jsonの完全化
  - デバイスメーカーとSSAIプロバイダーは、デバイスの信頼性を検証する標準の開発と採用をサポートする必要があると考えられます（要求に対して暗号での署名など）。これは、デバイスの偽装と戦うための大きなステップとなるのです。

私たちは、このようなアクションに波及効果がある事を見てきました。問題に挙げられているスキームの収益性が低くなったときに、私たちのやってきた事に意味があり貢献できたと実感できるでしょう。悪意のある詐欺集団の収入を断ち切ることにより、彼らをエコシステムから追い出すことができるようになります。ホワイトオプスの広告インテグリティは、私たちが協力しているパートナーの助けを借りて、集団的に保護された広告サプライチェーンを提供し、広告主がCTVやインターネット上で最も高度なボット攻撃の犠牲にならないように役割を果たします。

付録

オペレーションのトラフィックソースとして識別された

White Ops

ASNのサブセット：

29182
49392
51167
51659
59729
203004
204490
204601
204957

ICEBUCKET以外のトラフィックも存在するため、ASNからの全てのトラフィックがICEBUCKETオペレーションの一部であるとは限りません。

存在するユーザーエージェント：icebucket-uas.txt
含まれている全てのユーザーエージェントがICEBUCKETオペレーションに対して特有　であるとは限りません。このオペレーションは正当なトラフィックのように見えるようにされているため、オペレーション外部で見えるデバイスもここに表示されています。

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.