# 3ve の調査

## 業界のコラボレーションを通じて、主要な広告詐欺行為を防止

2018 年 11 月
Google と White Ops の共著
Proofpoint などによる技術支援

### 序文

毎年、サイバー犯罪に新しいレベルの精巧さとイノベーションがもたらされており、昨年も例外ではありませんでした。

昨年を通して、私たちはこれまでに見てきた中で最も複雑で精巧な広告詐欺の 1 つを調査しました。この詐欺行為を「3ve」（「イブ」と発音）と名付け、その調査活動から学んだことをより広範なコミュニティーと共有して、現在のサイバー犯罪との戦いで協働することを促進しています。これらの取り組みは、デジタル広告業界全体で効果的な協力とコラボレーションが広告詐欺をいかに抑制することができるかを示しています。

3ve は大規模なスケールで遂行されました。ピーク時には、主に北米とヨーロッパで住宅ボットネット感染と企業 IP スペースの両方から 100 万以上の IP を制御しました（これはアイルランドのブロードバンドサブスクリプションの数を超えています）。それはいくつかのユニークなサブオペレーションを特徴としており、それぞれが独自の精巧な広告詐欺スキームを構築しました。3ve の遂行をホストするために使用される大規模インフラストラクチャ（多くのデータセンターにある数千のサーバーで構成される）を識別し始めた直後、マルウェアに感染した住宅用コンピューターのネットワーク内で同様のアクティビティが発生していることがわかりました。これらの多様化された戦術とサイロ化された詐欺行為により、3ve のオペレーターは以前に遭遇した詐欺行為よりも識別が難しくなり、1 つのアスペクトが中断されたとしても大規模な詐欺企業は存続できました。その多様で複雑な機械を通じて、3ve は何十億もの不正な広告入札リクエスト（つまり、広告主が自動で入札して購入できる Web ページ上の広告スペース）を生成しました。

3ve のサイズと戦術は、広告詐欺の運用にはかなり重要ですが、詐欺師が複雑な広告詐欺スキームの開発に時間と労力を費やしているという事実は驚くことではありません。広告詐欺は収益性が高く、比較的低リスクのため、魅力的なサイバー犯罪なのです。ほとんどの詐欺師にとっての主要リスクは、詐欺行為が見つかり、シャットダウンされることです。これにより、詐欺師は数千ドル、場合によっては数百万ドルの不正な利益を得ることができますが、純粋な金銭的な見込み損失は、詐欺師が別の詐欺行為に手を出すことを抑止するほどのものではありません。

今日、3ve により完全に立ち向かい、解体することを可能にするための共同の取り組みの集大成です。調査結果を法執行機関に報告し、今日、米国司法省が 3ve の行為に関連する刑事告発を発表しました。その後、法執行機関と、アドテク、サイバーセキュリティ、インターネットサービスプロバイダーを含む業界のさまざまな企業の双方が、インフラストラクチャとシンクホールボットネットのコマンドアンドコントロールサーバーを無効にするための協調的かつ協調的な取り組みを行いました。これまでの結果により、詐欺行為のボットネットは不正な広告トラフィックを継続的に駆動できなくなりました。マルチステークホルダーワーキンググループのコンテキストで 3ve のような詐欺行為の多くのターゲット（顧客を含む）を守るには献身、勤勉さ、および忍耐が必要でした。私たちの主な

目的は、お客様とインターネットユーザーに代わってこの詐欺を発見および防止し、この行為を利益源から切り離すことでした。

広告詐欺は引き続き広告業界の課題となっていますが、今日行われている措置は、詐欺師にとって深刻な結果を招く可能性のある危険な行為であることを示しています。そして、私たちの取り組みはこれで終わりではありません。デジタル広告経済の整合性を保護するための業界全体の動きは今後も続くと確信しています。

## コンテキストと背景

データサイエンスとサイバーセキュリティの世界は、映画の探偵のようなものではありません。通常、不正行為が特定され、その発信元まで追跡されてから遮断されます。これで、大部分のケースが終了します。企業の広告詐欺防止が刑事告発につながることはめったにありませんが、それはまさに 3ve で起こったことです。

3ve は当初、小さなボット主導の取り組みとして出現し、その後、大きく精巧な詐欺行為に成長しました。私たちが調査し、それと対峙していくうちに、詐欺行為とその積極的な進化をさらに理解し始めました。そして、いくつかの共通の特徴を持つ行為がいくつかあることに気付きました。私たちの「戦い」を通じ、発見と探訪、そして冒険と呼ばれても相違ない道にいることがわかりました。

今日、デジタル広告は主に「プログラマティック」プラットフォームを通じて売買されています。パブリッシャーは、コンテンツと一緒に広告を掲載し、サプライサイドプラットフォーム（SSP）を使用して、利用可能な広告スペースまたは在庫を広告主にオークションすることに同意します。広告主は、デマンドサイドプラットフォーム（DSP）を使用して、それらの広告がどれくらい訪問者の関心を引くことができるかに基づいて、利用可能な広告スペースに入札します。これらのオークションは、ページがブラウザに読み込まれるまでのミリ秒単位で 1 日に数十億回行われ、画面に広告を掲載したい広告主とマッチングする前に、多くのオークション間で在庫を渡すことができます。

プログラムでデジタル広告在庫を販売および購入できるため、パブリッシャーは収益を最大化し、広告主は投資収益率を高めることができました。その後、プログラマティック広告は急速に進化し、数十億ドル規模の業界へと成長し、デジタル広告エコシステム全体で注目度と可視性をますます獲得しています。残念なことに、この注目度の高まりは、広告に実際の関心のあるユーザーに見られていると信じ込ませるために、偽のトラフィックや詐欺的な広告インベントリを作成しようとするハイテクに精通した詐欺師の注目を集めています。これらの詐欺師は、損失を無縁のように見せることを目的として、複数の当事者や取引から小額のお金を搾取しようとします。成功した場合、これらの搾取額は詐欺師にとってかなりの利益になります。

3ve のような詐欺行為は、デジタル広告エコシステムに不信と不安定をもたらすため、可能な限り徹底してダウンさせるよう尽力しました。その後紆余曲折があり、詐欺師が被害者とその活動を明らかにしようとする者の両方の告発を逃れるために使う戦術とアプローチに関する貴重な教訓と、将来的に同様の活動につながるヒントについて学びました。

## 斬新で革新的な広告詐欺の脅威

3ve は、広告主からの需要が高い 2 つの主要な資産の偽造品を販売することで収益を生み出したという点で、多くの広告詐欺操作の典型でした。視聴者とプレミアムパブリッシャーの広告枠です。しかし、3ve は一流のパブリッシャーのドメインを偽造し、大量のボットを偽の在庫に送信するのに非常

に効果的だったため、大量の偽の広告入札リクエストを生成することができました。3ve は、一連の無関係な行為であると思わせる精巧さで機能しました。そのオペレーターは 3ve のボットを偽装するために常に新しい方法を採用しており、トラフィックがブラックリストに登録されたとしても詐欺行為を拡大し続けています。1 か所でブロックされるたびに、どこか別の場所に再表示されるのです。

3ve は、広告主からの需要が高い 2 つの主要な資産の偽造品を販売することで収益を生み出したという点で、多くの広告詐欺操作の典型でした。視聴者とプレミアムパブリッシャーの広告枠です。

広告詐欺から身を守るために、業界は White Ops のようなサードパーティの検証ソリューションと、Google が実装するような社内防御に依存しています。まとめて、私たちのチームは、幅広いボットネットスキーム、広告詐欺の戦術、および無効なアクティビティを見てきました。

この知識と専門性は、3ve の深度調査を遂行し、そのすべての異なるサブオペレーションとコンポーネントをより大きなインフラストラクチャに繋ぎ、これらの詐欺行為がいかに洗練され、よく組織化されているかを明らかにするのに役立ちました。

**3ve オペレーション**

典型的な広告詐欺行為は、利益モデルをシンプルに保ち、デジタル広告エコシステムの 1 つの側面のみを対象としています。たとえば、詐欺師は通常、ボットトラフィックを作成して、コンテンツに目を向けようとしている疑いを持たないパブリッシャーに販売します。3 つの 3ve サブオペレーションのうち少なくとも 2 つがこのような戦術を使用し、別の一般的なアプローチも足していました。3ve のオペレーターによって「なりすまし」された人気ウェブサイトのドメインをフィーチャーした偽造広告枠を販売する方法です。ドメインスプーフィングは、広告の印象が、有名な新聞のようなプレミアムサイトに掲載されたと思わせるように設計されています（ボットトラフィック用に設計された空の Web サイトではありません）。

ただし、これは実際には 3 つの異なるサブオペレーションのセットの背後にある基本的な前提のみを説明し、それぞれが検出を回避するための独自の手段を取り、それぞれが異なるコンポーネントを使用して異なるアーキテクチャを中心に構築されています。完全に専門的なソフトウェア会社のように、3ve のオペレーターは、さまざまなアプローチとボット操作のさまざまな部分を A / B テストして、一部が何らかの理由で切断またはシャットダウンされた場合にフォールアウトから身を守ることができました。3 つのサブオペレーション間で複雑さの程度は異なりますが、3 つすべてが実際の人間ユーザーのなりすまし、タグ回避、マルウェアベースの高度なアンチフォレンジックなど、非常に高度な動作を示しました。

組み合わされた 3 つの 3ve サブオペレーションは、これまでに発見されなかった最も広範囲に及ぶ広告詐欺行為の 1 つでした。3 つのサブオペレーションのうちの 1 つには、任意の時点で最大 700,000 のアクティブなデスクトップ感染を伴う、より大きなアクティブなボットネットの 1 つが含まれていました。他の 3ve サブオペレーションの 1 つは、2016 年の Methbot オペレーションとサイズおよび範囲がそれ自体で類似しており、おそらく当時で最もよく知られた広告詐欺オペレーションでした。

全部で、3ve は住宅ボットネット感染と企業 IP スペースの両方から 100 万個以上の IP を制御しました（上記のように、常に最大 70 万件のアクティブな感染がありました）。全体として、このオペレーションは 10,000 を超える偽造ドメインを生成し、ピーク時に毎日 30 億を超える入札リクエストを

生成しました。ボット操作の部分は、このタイプの大規模オペレーションに必要なさまざまな機能に割り当てられたデータセンターの 1,000 台を超えるサーバーにまたがっていると推定されます。

3ve の規模と積極的な成長にもかかわらず、私たちは顧客を保護し、3ve のオペレーターがそのアクティビティから利益を得る可能性を減らすために、積極的に対策を展開しました。広告詐欺との闘いにおける私たちのまとまった経験により、3ve を解体するために並行して取り組みながら、3ve に対してさまざまな防衛策を確立することができました。