infoblox

Threat Intel

DNS プレデター攻撃：VIPERS と HAWKS が乗っ取る SITTING DUCKS ドメイン

著者
Infoblox Threat Intel

目次

はじめに

それは類似ドメインから始まりました。このドメインは Slack ホスティングリソースそっくりに作成されていましたが、実際にはロシアでホストされていました。単純なフィッシングでしょうか？そうかもしれません。ただし、奇妙なリダイレクトチェーンを除けばですが。長い間登録されていた CBS Interactive ドメインが、潜在的な被害者を偽の Slack ポータルにリダイレクトするために使用されていました。[1] テレビ局は本当にドメインを削除したのでしょうか？いいえ、ドメインは Mark Monitor に登録されたままでした。しかし、DNS の名前解決の履歴を確認すると、しばらくアイドル状態だったドメインがロシアで名前解決され始めたことは明らかでした。乗っ取られたに違いありません。2024 年 1 月当時、`clickermediacorp[.]com` のような価値の高いドメインを乗っ取ることは、認証情報の盗難の兆候であると考えられていました。私たちはドメイン登録事業者と DNS プロバイダーの両方にこの乗っ取りについて報告し、先に進みました。

数か月後、謎のドメイン乗っ取りの話題が再び浮上しました。Proofpoint の研究者は、マルウェアやその他の悪意のあるコンテンツの配布に関連する 404TDS と呼ばれる犯罪トラフィック配信システム（TDS）を追跡していました。私たちの専門分野は DNS の脅威検出です。他社がマルウェアをリバースエンジニアリングしたり、Web ページを解析したりするのに対し、私たちは DNS レコードの構成方法や操作後に残るクエリの痕跡から攻撃者のフィンガープリント（痕跡）を見つけます。TDS は本質的に DNS 構成に組み込まれているため、悪意のあるペイロードを待つのではなく、TDS の進化を監視できるパターンを頻繁に確認できるため、TDS アクターは私たちにとって非常に有益です。私たちは、404TDS の DNS 署名があるに違いないと考えました。

1 https://urlscan.io/result/8ee644c6-2ad3-4cd9-a0e6-e05ad01ade5d/

404TDS を追跡する仕組みを探し始めると、clickermediacorp[.]com を含むすべてのドメインが乗っ取られていることがすぐに明らかになりました。しかし、これらの乗っ取りの範囲は異常に広く、認証情報の盗難や登録事業者のハッキングの仕業では説明がつきませんでした。私たちは Eclypsium の研究者と協力し、404TDS につながっている広範なドメイン乗っ取りの真相解明を始めました。

DNS ネームサーバーの設定ミスがすべての乗っ取りでの共通要因であり、ボタンを数回クリックするだけで特定のプロバイダーの誤って構成されたドメインを乗っ取ることができることがわかりました。私たちは DNS 脅威の専門家ですが、これは私たちにとって初めての経験でした。これは私たちだけでなく、2024 年 7 月に出版する前に、政府機関や産業界、脅威研究やネットワークに携わる幅広い人々も同じでした。最初の数か月間、私たちが話をした人は誰も攻撃ベクトルに気づいていませんでした。もちろん、その大量搾取についても知りませんでした。Brian Krebs 氏は、この手法を使った大規模なキャンペーンを取り上げたことを覚えていました。しかし、Krebs 氏が報告した時点では、それはシステム全体の問題ではなく、1 社のドメイン登録事業者だけの問題のように見えました。[2] 私たちはついに、Matt Bryant 氏によるこの脆弱性に関する最初の報告（私たちが「Sitting Ducks」と名付けた）を発見し、アクターがこの攻撃ベクトルを少なくとも 8 年間、検出されることなく使用していた可能性が高いことに気付きました。[3]

Sitting Ducks に関する最初の論文は、あまり知られていない乗っ取り手法に対する認識を高め、ドメイン所有者と登録者がドメインを保護するために取るべき具体的な行動を示すことを目的としていました。犯罪者だけでなく、行動を促すことを期待していました。調査の結果、これらの脆弱なドメインは、合併、買収、人事異動による履歴の消失などによって生じることが多いことがわかりました。clickermediacorp[.]com ドメインは 7 月のレポート後に保護されましたが、残念ながら他の CBS ドメインは脆弱なままです。この *Paramount Global* をお読みで支援が必要な場合は、お気軽にご連絡ください。被害を受けたある組織と協力してドメインを修復しました。被害を受けた組織はドメインに関する情報だけでなく、ドメイン登録事業者の認証情報も失っていたためです。最も憂慮すべきケースでは、.gov の所有者と協力して構成を修正しました。

最初の公開以来、私たちは約 80 万の脆弱な登録ドメインを特定しました。その後、脆弱なドメインの約 9%（70,000）が乗っ取られました。これらの数値は限られた監視システムから導き出されたもので、攻撃対象領域を正確に反映していないことはわかっています。Sitting Ducks 攻撃の課題は、実行が簡単である一方、検出が非常に難しいことです。サイバー犯罪者は、少なくとも 2018 年からこの攻撃ベクトルを利用して、有名ブランド、非営利団体、政府機関が所有するドメイン名を含め、8 万を超えるドメイン名を乗っ取っています。

今年見られた構成指向の攻撃ベクトルは、Sitting Ducks だけではありません。CNAME 乗っ取りには複数の種類があり、WHOIS サーバーの乗っ取りも報告されています。[4,5] 高位レベルでは、政府や標準化団体も、こうした種類の攻撃からユーザーを保護する役割を担っています。国内組織と多国籍組織はともに、DNS 乗っ取りなどの攻撃からの保護を組み込んだセキュリティ要件を含む、すべての構成関連の問題に対するリスクを軽減するための意識とインセンティブを高める必要があります。残念ながら、米国サイバーセキュリティ社会基盤安全保障庁（CISA）を含む多くの政府機関はソフトウェアの脆弱性に重点を置いているため、構成の脆弱性が潜在的に犯罪的なインパクトがあるにもかかわらず、この脆弱性は CVE の指定対象になりません。たとえば、.gov の登録者でさえ TLD では、「有能な」DNS プロバイダーを使用する必要があるだけです。その結果、特定の登録事業者が、DNS プロバイダーのレコードが確立される前にネームサーバーの設定を強制することで、新しいドメイン登録で委任されているにもかかわらず、適切に情報を返さない、正しく委任できていない状態（lame delegation）であることがわかりました。これは時間との競争ですが、私たちは何度もそれを観察してきました。こうした問題に対する注意が欠如しているため、脆弱性攻撃はほとんど衰えることなく続いています。願わくば、Sitting Ducks 攻撃ベクトルだけでなく、構成の脆弱性全体に対処するための意識向上トレーニングと予防的対策の両方が開発され始めることを期待します。

2 https://krebsonsecurity.com/2019/01/bomb-threat-sextortion-spammers-abused-weakness-at-godaddy-com/

3 https://thehackerblog.com/floating-domains-taking-over-20k-digitalocean-domains-via-a-lax-domain-import-system/

4 https://labs.guard.io/subdomailing-thousands-of-hijacked-major-brand-subdomains-found-bombarding-users-with-millions-a5e5fb892935

5 https://labs.watchtowr.com/we-spent-20-to-achieve-rce-and-accidentally-became-the-admins-of-mobi/

あまりに一般的な反応は、ドメインの構成を維持する最終的な責任をドメイン保有者に押し付けることです。それは否めないことかもしれませんが、同時に、登録事業者と DNS プロバイダーの両方が、この種の乗っ取りを実行しにくくしたり、修復しやすくしたりすることで、サイバー犯罪を減らす上で重要な役割を果たすことができます。調査中、Sitting Ducks の乗っ取りを登録事業者と DNS プロバイダーの両方に報告しましたが、攻撃の証拠を提供したにもかかわらず、ほとんど退けられ、対策も講じられませんでした。多くの場合、ドメイン所有者が非公開の登録情報を使用していたため、ドメイン所有者に通知することができませんでした。侵害されたドメイン所有者とやり取りした複数のケースでは、自分たちがドメインの所有者であること、時間の経過や企業合併によってメモリや文書が失われたことに気づいていませんでした。ドメイン所有者に連絡できないということは、現実的には、犯罪を減らすためには、登録事業者と DNS プロバイダーの両方が、脅威情報機関などからの情報への対応においてより積極的な役割を果たし、プラットフォームやユーザーの悪用を最小限に抑える必要があります。

攻撃ベクトルを調査しているうちに、それを悪用している独立したアクターが十数人いることがわかりました。このホワイトペーパーでは、404TDS と VexTrio Viper の運営者を含め、そのいくつかの事例について説明します。また、私たちが追跡する 2 つの新しいアクター、Horrid Hawk と Hasty Hawk もご紹介します。

このホワイトペーパーの目的は、これらの乗っ取られたドメインをより簡単に特定してシャットダウンできるようにするための具体的な方法を示すことです。次のことを共有していきます。

- Sitting Ducks 攻撃を回避し、侵害されたドメインを特定する方法
- さまざまな脅威アクターが Sitting Ducks 攻撃を利用して、セキュリティベンダーの検出に強いインフラストラクチャを構築している方法
- Sitting Ducks の脅威アクターが互いに協力し合っている様子や乗っ取ったドメインについてのある種の共有情報または地下組織の経済を示すこと
- 大手ブランドに関連する一部のドメインが、多くの場合別の脅威アクターによって繰り返し乗っ取られている様子
- DNS がこれらの執拗な脅威アクターの検出と追跡において中心的な役割を果たす理由

SITTING DUCKS 攻撃ベクトル

まずは要約から始めます。7 月に、私たちは Eclypsium と共同で、広く悪用されながらもあまり報告されていない「Sitting Ducks」と呼ばれる攻撃ベクトルに関するレポートを発表しました。[6] この攻撃では、悪意のあるアクターはドメインの DNS 構成を制御することで、ドメインの完全な制御権を獲得します。また、ドメイン所有者の登録事業者アカウントにアクセスすることなくドメインを巧妙に乗っ取ることもできます。ほとんどの場合、これらのドメインやサブドメインは元の所有者に忘れられているため、攻撃は気づかれません。このように乗っ取られたドメインを悪用して、マルウェアの配布、コマンド＆コントロール（C2）、フィッシング、トラフィック配信システム（TDS）の運用など、さまざまな犯罪行為を行う十数におよぶ脅威アクターを確認しています。

Sitting Ducks 攻撃は、ドメインの DNS 設定の誤った構成、具体的には DNS が誤った権威ネームサーバーを指している場合に利用されます。攻撃者がこの方法でドメインを乗っ取るには、いくつかの条件を満たす必要があります。

登録済みドメインまたは登録済みドメインのサブドメインが、ドメイン登録事業者とは異なるプロバイダーに権威 DNS サービスを使用または委託している、これを**委任**と呼びます。

- 委任が**正しく行われていない状態**である、つまり、レコードの権威ネームサーバーにはドメインに関する情報がなく、クエリを解決できない。
- 権威 DNS プロバイダーは**悪用可能**であり、攻撃者はプロバイダーでドメインを「要求」し、ドメイン登録事業者の有効な所有者のアカウントにアクセスすることなく DNS レコードを設定できる。

6 https://blogs.infoblox.com/threat-intelligence/who-knew-domain-hijacking-is-so-easy/

図 1 は、一般的な Sitting Ducks 攻撃の一連の流れを示しています。このタイプの攻撃にはいくつかのバリエーションがありますが、いずれも正当な DNS インフラストラクチャを侵害する必要がないため、よく知られている DNS 乗っ取り手法とは根本的に異なります。この攻撃のバリエーションには、別の DNS プロバイダーへの再委任や、部分的に正しくない状態の委任（権威ネームサーバーの一部のみが誤って構成されている）が含まれます。技術的な参入障壁が低いため、さまざまなサイバー犯罪グループがこの脆弱性を悪用する機会を得ています。その結果、乗っ取られたドメインの多くが良い評判を持っているため、検出が困難な攻撃事例が増えます。

Sitting Ducks の攻撃は簡単に実行でき、検出が難しいですが、ドメイン登録事業者と DNS プロバイダーで正しく設定すれば完全に防ぐこともできます。ただし、すべての DNS プロバイダーが悪用されるわけではありません。約 12 件のプロバイダーを評価した結果、悪用可能なプロバイダーで毎日何百ものドメイン乗っ取りが発生していることを確認しました。8 月以降、約 80 万個の登録ドメインが正しくない状態の委任を受けていることが確認されましたが、これには脆弱なサブドメインは含まれておらず、検索対象を特定のプロバイダーに限定しているため実際の数ははるかに多いです。

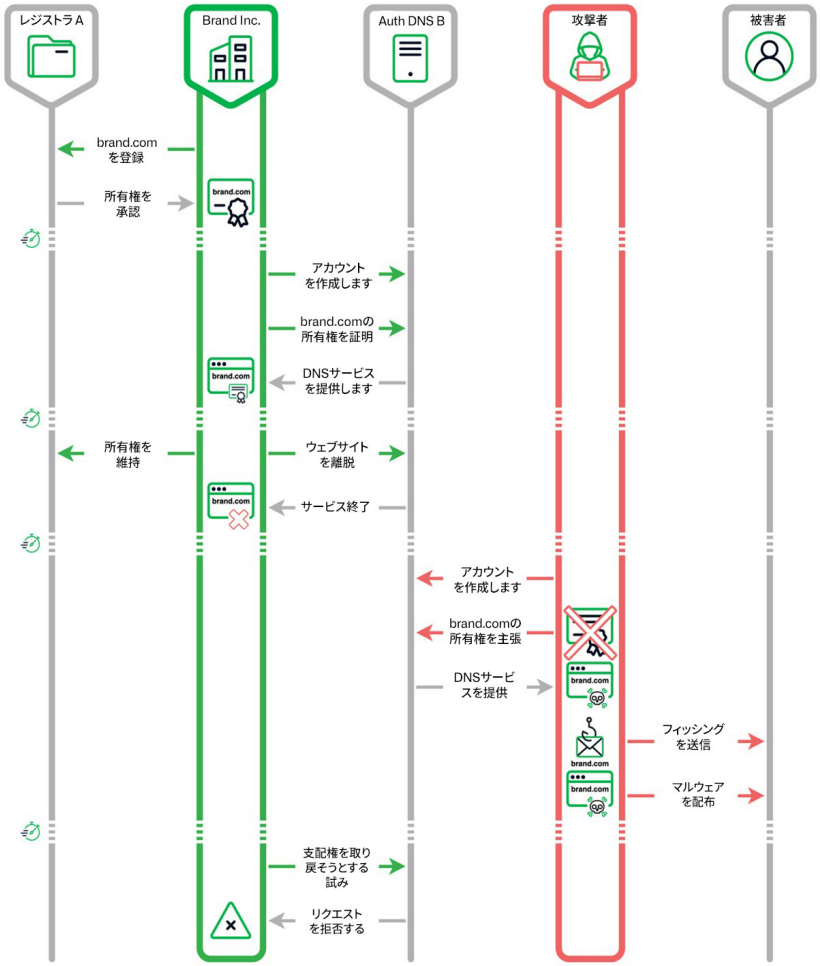

図 *1. Sitting Ducks* の一般的な攻撃の流れ

脅威アクターがプロバイダー間で脆弱なドメインをどのように特定するかはまだ不明です。複数の検出方法を実装しましたが、それらを通じて、特定の日に悪用可能な DNS プロバイダーに割り当てられたドメインの 6 ～ 10% の委任が正しくない状態であることがわかりました。悪用可能なプロバイダーの中には、非常に多くの脆弱なドメインを持っているものもあり、私たちのテストが限られていたことを考えると、実際に悪用される可能性のある状況はおそらく今日私たちが知っているよりもはるかに大きいでしょう。全体として、1 日に 100 万を超える登録ドメインが Sitting Duccks の攻撃に対して脆弱であると推定しています。私たちが発見した最も脆弱なドメインでは、少数の DNS プロバイダーのいずれかにネームサーバーが割り当てられています。

ここで、この攻撃ベクトルを使用するアクターの一部を見てみましょう。

VACANT VIPER

「名前」には何が含まれているのか？

Vacant Viper は、Proofpoint によって最初に報告された 404TDS を運用する脅威アクターに私たちが付けた名前です。[7] 慣例として、Infoblox は、実証されているアクターやインフラストラクチャのコンポーネントの名前を変更しません。404TDS について言及する場合は、TDS 自体について議論しており、Vacant Viper について言及する場合は、404TDS のドメインを乗っ取り、スパムなどの他の悪意のある活動に従事するアクターについて議論しています。

ドメインが TDS インフラストラクチャの一部になることを予測できる DNS 署名を探して 404TDS を調査していたところ、ドメインが乗っ取られていることに気付きました。さらに、侵害されたドメインを注意深く見ると、アクターは単に犯罪的な TDS を運用する以上のことをしているようでした。私たちは、TDS の起源であることを認め、危険人物カテゴリを使用して、乗っ取り攻撃アクターを Vacant Viper と名付けました。

Vacant Viper は、Sitting Ducks を悪用した最も初期の既知の脅威アクターの 1 つで、2019 年 12 月以降、毎年推定 2500 個のドメインを乗っ取っています。このアクターは、乗っ取ったドメインを使用して、悪意のあるスパム運用を実行したり、ポルノを配信したり、リモートアクセス型トロイの木馬（RAT）C2 を確立したり、404TDS 運用に加えて、DarkGate や AsyncRat などのマルウェアを投下したりします。[8] 報告されているアフィリエイトには TA-866 と TA-571 が含まれています。

Vacant Viper は DigiCert DNS 利用企業を悪用しますが、DNS Made Easy の無料アカウントを好んでいます。このアカウントは 30 日間の試用期間があり、設定に必要なのはメールアドレスだけです。しかし、無料トライアルの前に営業担当者との連絡が必要なプレミアム DNS サービスである Constellix のドメインも乗っ取っています。2024 年 7 月に初めて Sitting Ducks 攻撃について報告して以来、アクターは手法を調整していますが、引き続きこのプロバイダーセットのみで活動し続けています。彼らが行う乗っ取りの量は時間とともに変化しますが、たとえば、2024 年 10 月の最初の 2 週間で、Vacant Viper によって乗っ取られたドメイン数は約 100 個であると特定しました。

Vacant Viper は、特定のブランドに接続するためにドメインを乗っ取るのではなく、評判が高く、セキュリティベンダーによってブロックされないリソースのセットを乗っ取っています。また、Vacant Viper は、いくつかのドメインを長期にわたって繰り返し乗っ取っています。たとえば、`clickermediacorp[.]com` は、2024 年 1 月に 404TDS の一部として確認され、Slack を模倣したフィッシングキャンペーンに関連していましたが、このドメインは以前、2020 年 1 月にポルノやビットコイン詐欺など、さまざまなコンテンツを配信するために使用されていました。

7 https://www.proofpoint.com/us/blog/threat-insight/screentime-sometimes-it-feels-like-somebodys-watching-me

8 https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta571-delivers-icedid-forked-loader

TDS の主な特徴は、アフィリエイト（TDS にトラフィックを送信するサプライヤーと、TDS からトラフィックを受信する顧客）が存在することです。広告業界における TDS の目標は、利益を最大化すること、つまり、ユーザーが最も好む可能性の高い広告にユーザーを誘導することです。犯罪 TDS の目的も同様です。つまり、ユーザーが最も利用したいと思うコンテンツでユーザーを誘い込み、マルウェアのダウンロード、偽のログインページ、ギフトカード詐欺などの悪質なコンテンツに誘導することです。

次の 404TDS 攻撃チェーンの例は、Vacant Viper が 404TDS で乗っ取ったドメインを使用する方法など、TDS とそのアフィリエイトの両方が使用するリダイレクト手法を示しています。

Vacant Viper が乗っ取り 404TDS で使用したドメインの 1 つは mcpennsylvania[.]com です。これは、McDonald が企業ドメイン登録事業者の CSC Corporate Domains に登録し、DigiCert の子会社である DNS Made Easy のネームサーバーに割り当てられたドメインです。[9] Vacant Viper は過去数年にわたってこのドメインを繰り返し乗っ取り、この記事の執筆時点では委任が正しくない状態です。最近では、この McDonald のドメインが ncbtv[.]com（以前は IPTV サービスプロバイダーが運営）にリダイレクトされているのを確認しました。このドメインは 2011 年に GoDaddy に登録され、当初は中国のメールアドレスで登録されていました。皮肉なことに、このドメインも現在はプライベート登録の対象になっていますが、Sitting Ducks 攻撃によって、おそらく 2017 年頃から複数回乗っ取られたようです。最近では、ncbtv[.]com は、乗っ取ったドメインを使用して出会い系サイトやその他のコンテンツをホストする脅威アクターである VexTrio Viper と関連付けられています。このアクターが Vacant Viper とは無関係であると仮定すると、Sitting Ducks 攻撃を使用する脅威アクターは互いに協力し、脆弱なドメインに関する知識やリソースを共有している可能性が高いことがわかります。

2023 年 6 月、Vacant Viper が mcpennsylvania[.]com を乗っ取った際、AsyncRAT マルウェア攻撃チェーンの 404TDS に Sitting Ducks 攻撃を使用し、2 つの異なるメカニズム（メタリフレッシュと HTTP リフレッシュ）を活用してユーザーをリダイレクトしました。[10]

URL の hXXps://mcpennsylvania[.]com/y0t/gojhuovy は 404（Not Found）エラーを表示しましたが、裏ではメタリフレッシュが実行され、HTML メタタグを介してユーザーをリダイレクトしました。

» <meta http-equiv=”refresh” content=”0;hXXps://ecole-artcom[.]com/wdown」 >

- 2 番目の URL hXXps://ecole-artcom[.]com/wdown/ は、リフレッシュ HTTP ヘッダ以外のコンテンツなしで応答しました。これは、ユーザーを再び 3 番目の URL に効果的にリダイレクトしました。
- 3 番目の URL hXXps://www[.]mediasimulasi[.]com/wazxd は、Information_28_jun_1220107.js という JavaScript ファイルを投下し、AsyncRAT に関連するファイルのダウンロードへと進みました。[11]

ランディングドメインを誰が制御しているかは不明ですが、404TDS との関連でのみ確認されています。図 2 は、mcpennsylvania[.]com 攻撃チェーンのヘッダーを示しています。

9 https://who.is/whois/mcpennsylvania.com

10 https://urlscan.io/result/14797fe3-beaf-4949-9d04-6edcf94b25aa/#transactions

11 https://github.com/executemalware/Malware-IOCs/blob/main/2023-07-05%20AsyncRAT%20IOCs

図 2. ヘッダーをリフレッシュすると、ユーザーは hXXps://www[.]mediasimulasi[.]com/wazxd にリダイレクトされます。

Vacant Viper は、悪意のあるスパム添付ファイルを通じて DarkGate マルウェアを配布する攻撃チェーンでも HTML メタリフレッシュ手法を使用しました。DarkGate マルウェア配信のリダイレクトチェーンは、[12] AsyncRAT の場合と似ていますが、HTTP リフレッシュ手法は含まれていません。

1. ユーザーが afarm[.]net にアクセスしようとすると、404 Not Found エラーが発生します。
2. TDS URL hXXps://afarm[.]net/uvz2q は、HTML メタリフレッシュ手法（<meta http-equiv=”refresh” content=”0;hXXps://wercosliuhqgheirn[.]com/”>）を介して https://wercosliuhqgheirn[.]com/ にリダイレクトされます。
3. ユーザーは hXXps://moarhofhechtl[.]at/wp-content/plugins/image-hover-effects-addon-for-elementor/download[.]php にリダイレクトされ、DarkGate マルウェアを含む以下のファイルをダウンロードします。

ファイル名	SHA-256 ハッシュ
08-May-24-document-53aa77b6.jar	f20585b7183d6380968b8f1d75a34bb78b6224e5686ebb81430ec14e80fce17a

表 1 の 8 個のドメインはすべて同じリダイレクトパターンに従って、DarkGate に関連する同じ JAR ファイルを配信します。[13] 2024 年 5 月には、may-document_85138492.pdf など、同様の名前のスパム添付ファイルに、これらのドメインの 6 個を確認しています。これらのファイルはすべて、悪意のあるスパムメールの添付ファイルとして配布され、添付された請求書や経費明細書を参照する同じような一般的な本文メッセージで、ユーザーが支払いを行うために開くように促しています。

aerospaceavenue[.]com	affiliatebash[.]com
affixio[.]com	amikamobile[.]com
adventsales[.]co[.]uk	afcmanager[.]net
afarm[.]net	adztrk[.]com

表 *1. DarkGate* マルウェアを配布するために *Vacant Viper* が使用した乗っ取られたドメイン

12 https://urlscan.io/result/1f4d4a62-8a6f-4452-b64c-1d38b3cd6086/#summary

13 https://bazaar.abuse.ch/sample/f20585b7183d6380968b8f1d75a34bb78b6224e5686ebb81430ec14e80fce17a#intel

Vacant Viper の調査により、Sitting Ducks 攻撃ベクトルが（再）発見されましたが、他の脅威アクターをその攻撃ベクトルに結び付けることもできました。これらのアクターの中には追跡されているものもあれば、追跡されていないものもありました。一般的に、侵害されたドメインをそれ自体で発見することは非常に難しいことがわかりました。脅威アクターの行動を利用して、追跡可能な署名に戻りました。DNS 乗っ取りを利用する脅威アクターについては、Hawk（タカ）の命名カテゴリを使用しています。

なぜタカなのか？

これらの脅威アクターは、タカが獲物を捕まえるために潜り込むのと同じように、脆弱なドメインに急襲して乗っ取ります。

HORRID HAWK

Horrid Hawk は、少なくとも 2023 年 2 月以降、ドメインを乗っ取って投資詐欺に使用している DNS 脅威アクターです。この脅威アクターは最近のキャンペーンのあらゆる段階で乗っ取ったドメインを使用し、存在しない政府の投資プログラムやサミットについて説得力のある誘惑を仕掛けているので、興味深いです。彼らは乗っ取ったドメインを短時間の Facebook 広告に埋め込み、複数の大陸にまたがる 30 以上の言語ユーザーをターゲットにしています。私たちは DNS を通じて Horrid Hawk を追跡し、乗っ取られたドメインを 5,000 個近く特定しました。

Horrid Hawk の攻撃チェーンには、2 つの異なる乗っ取られたドメインが関係しています。ほとんどの場合、これらのドメインは、Linode、TierraNet、A2 Hosting などのいくつかの DNS プロバイダーから乗っ取られています。ドメインを乗っ取った後、Horrid Hawk は A レコードの IP アドレスを別の専用サーバーに再構成します。アクターはドメインの 1 つを TDS サーバーに割り当てます。このサーバーは、ランディング Web ページをセキュリティ研究者から保護し、不要な Web 訪問者をフィルタリングします。Horrid Hawk は、もう 1 つのドメインを、詐欺的な投資コンテンツをホストするランディング Web ページに割り当てます。Horrid Hawk は、初期段階で、`oil-poland[.]site` や `balticpipe[.]playroom8[.]site` など、政府投資のテーマに一致する独自の類似ドメインも登録していました。このアクターは、ガスプロジェクト詐欺に関連するコンテンツをホストするランディング Web ページにこれらのドメインを使用しました。図 3 は、アクターが乗っ取り攻撃で一緒に使用した 2 つのドメインのタイムラインを示しています。

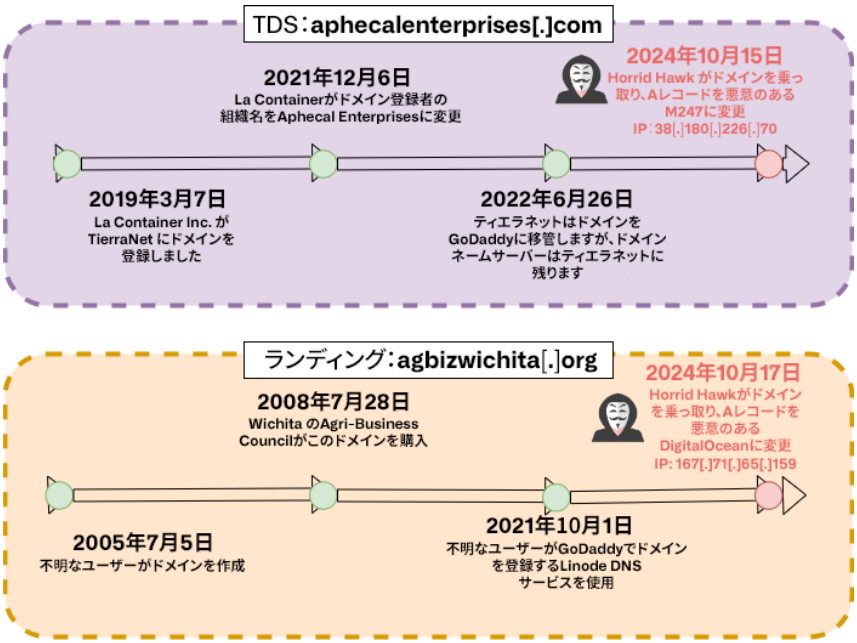

図 3. `aphecalenterprises[.]com`（*TDS*）と `agbizwichita[.]org`（ランディングページのドメイン）のドメイン乗っ取りのタイムライン

Horrid Hawk は、世界中の消費者を餌食にしています。彼らは、図 4 のような Facebook 広告を多数作成して攻撃を開始します。この広告はポーランドのユーザーをターゲットにし、政府が資金提供する偽のガスプロジェクトである Baltic Pipe プロジェクトを宣伝しています。Facebook 広告で使用された画像には、50 歳以上のユーザーに広告リンクをクリックしてウェブ記事の内容を読むように促すメッセージが含まれています。この Facebook 広告キャンペーンは 13,000 人を超えるインターネットユーザーに配信されました。このセクションで使用している例はポーランド語圏の中高年者ユーザーをターゲットにしたキャンペーンですが、Horrid Hawk は英語、イタリア語、トルコ語、スペイン語、その他多くの言語でもフィッシング詐欺をおこなっています。

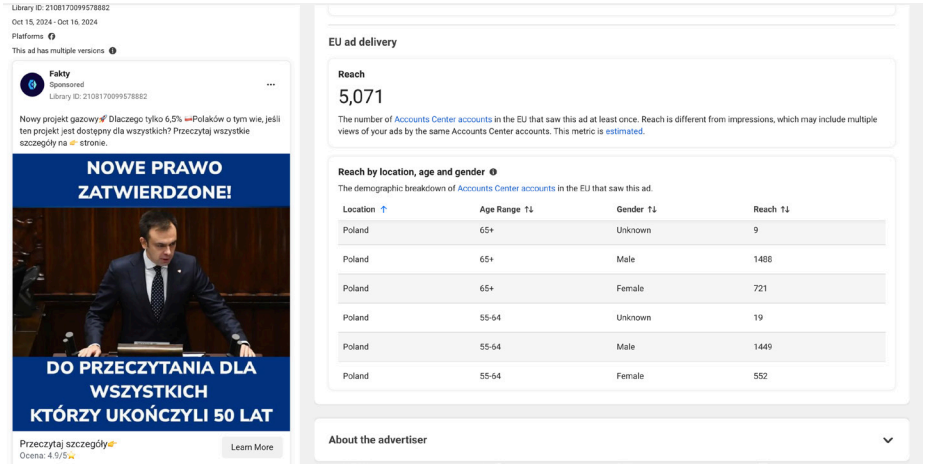

図 4. 主に 55 歳以上のポーランド語圏ユーザーをターゲットにした *Horrid Hawk* の *Facebook* 広告の例

図 4 に示す広告リンクは、Horrid Hawk TDS サーバーが使用した URL の `hXXps://aphecalenterprises[.]com/` を指しています。このシステムは、Web 訪問者をプロファイリングし、セキュリティ研究者や Web スクレイピングボットなどの無関係で不要なゲストをフィルタリングすることで詐欺ランディングページを保護するため、脅威アクターにとって重要です。サーバーは、地理位置情報を使用して、Web 訪問者の次の URL の場所を決定します。たとえば、ユーザーがポーランド拠点の IP アドレスから `hXXps://aphecalenterprises[.]com/` に移動すると、Horrid Hawk は、ユーザーを `hXXps://agbizwichita[.]org/9fMS3XSS` にある政府をテーマにした詐欺 Web ページにリダイレクトします。ランダム URL パス 9fMS3XS は一時的なもので、この Web サイトは、ベース HTML href 属性によって参照される静的ファイル（/lander/long-ready-2_0/index.html）を読み込みます。図 5 は、この URL がまだアクティブだったときに表示された Web ページです。

図 5. ポーランド語圏のユーザーをターゲットにした政治的テーマの詐欺ウェブページ（`hXXps://agbizwichita[.]org/lander/long-ready-2_0/index.html`）

ウェブサイト訪問者の IP アドレスが Horrid Hawk のターゲットユーザーとは無関係な国にある場合、それらのユーザーは通常、同じ TDS ドメインを使用するおとりの Web ページにリダイレクトされます。たとえば、ポーランド国外の IP アドレスで `aphecalenterprises[.]com` にアクセスしたときは、TDS はオンラインのアパレルストアを模倣した無害な Web ページを提供しました。図 6 は、おとりの Web ZX ページの URL 構造と内容を示しています。おとりの Web ページの URL には、静的プレフィックス `w-{country code}-` が付いたファイル名が含まれています。この場合の国コードは「pl」で、ターゲットとする国であるポーランドの略称です。「w」はおそらくホワイトカバーまたはホワイトラベルを表しています。

図 *6. Horrid Hawk TDS* がターゲット以外の *Web* 訪問者向けに提供するおとりの *Web* ページ

さまざまな Web ページで目にした最も頻繁に取り上げているテーマは、「The Baltic Pipe Project」に関するものでした。これは、ポーランド国民が新しいガスパイプラインに投資すれば巨額の利益が得られると主張する投資詐欺です。`agbizwichita[.]org` のランディングページに関する上記の例では、Horrid Hawk は人間の自然な「取り残される恐怖心（FOMO）」を利用した不安や恐怖心を煽る戦術を使用しています。この Web ページは、政府が資金を提供するガスプロジェクトに参加しない国民はガス関連の費用が 55% 増加すると主張しています。今年私たちが報告した別の投資詐欺アクターである Savvy Seahorse が運営する投資キャンペーンと同様に [14] Baltic Pipe キャンペーンでは、投資機会に登録するために、埋め込みフォームに名前、メールアドレス、電話番号などの個人情報を入力するようユーザーに求めています。その後、ユーザーは「投資プラットフォーム」にアクセスする前に、追加情報を求めて連絡が入ることが通知されます。　図 7 参照　他の脅威アクターも Baltic Pipe 詐欺を実行していますが、Horrid Hawk は、ドメインを乗っ取るために Sitting Ducks 攻撃を利用する点で際立っています。[15]

14 https://blogs.infoblox.com/threat-intelligence/beware-the-shallow-waters-savvy-seahorse-lures-victims-to-fake-investment-platforms-through-facebook-ads/

15 https://urlscan.io/result/61541987-122b-484d-acdc-290f02f98a8b/

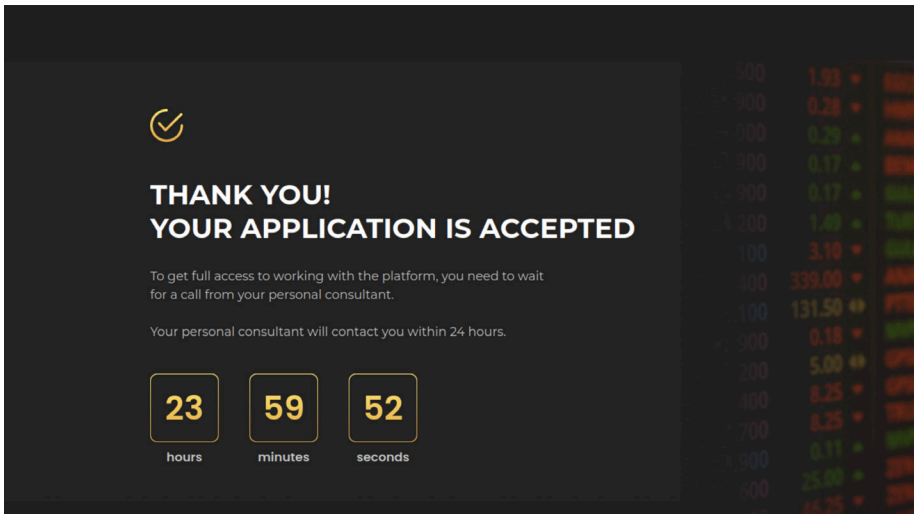

図 7. 被害者が詐欺サイトへの登録に成功した後に配信される典型的な *Horrid Hawk* からの応答ページ

ヘイスティホーク

Hasty Hawk は、Sitting Ducks の乗っ取りに関する調査中に発見したもう 1 つの脅威アクターです。少なくとも 2022 年 3 月以降、Hasty Hawk は 200 個以上のドメインを乗っ取り、主に DHL の配送ページやウクライナを支援するための偽の寄付サイトを偽装する広範囲なフィッシングキャンペーンを展開しています。このアクターは、HawkHost、Maria Hosting、DigitalOcean など、多くのプロバイダーを悪用しています。乗っ取られたドメインは、PROTON66 や BEGET などのロシアの ASN でコンテンツをホストするために DNS 経由で再構成されることがよくありますが、このアクターは OVH などの他のプロバイダーを利用することも知られています。Hasty Hawk は、Google 広告やスパムメッセージなどの他の手段を使用して悪意のあるコンテンツを配布します。

Hasty Hawk の完全修飾ドメイン名（FQDN）は、次のようないくつかのパターンに従う傾向があります。

- `dhl.< ランダムな数字 >.<hijacked domain>`
- `dhl-id< ランダムな数字 >.<hijacked domain>`
- `< ランダムな数字やアルファベット >.dhl.<hijacked domain>`

図 8 は、`thebagshelf[.]com` の DNS レコードの 作成日から Hasty Hawk に乗っ取られた日までの DNS レコードの変化を示しています。Horrid Hawk と同様に、Hasty Hawk も A レコードアドレスをアクター専用のサーバーに再構成します。`dhl[.]3204[.]thebagshelf[.]com` などの DHL サブドメイン名プレフィックスに加えて、これらのサーバーでは `id-f< ランダムな番号 >.<hijacked domain>`（例：`id-f0596[.]successbusinesspages[.]com`）などの他の静的サブドメイン名プレフィックスも確認されています。

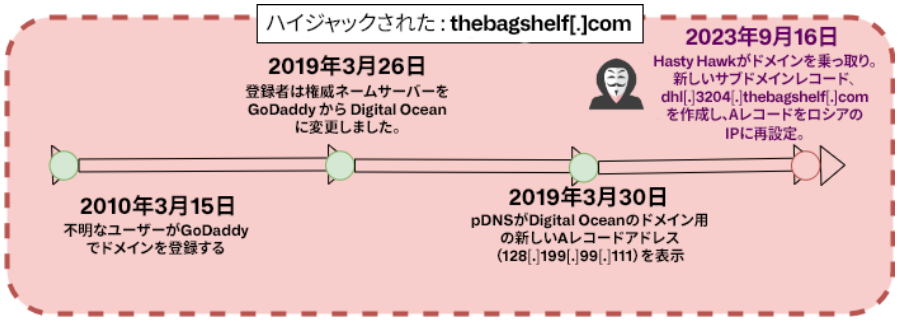

図 8. `thebagshelf[.]com` のドメイン乗っ取りのタイムライン

Hasty Hawk は最近、DHL をテーマにした Web ページの多くを、戦争中のウクライナを支援するため Global Shapers 組織が運営する正規サイト supportukrainenow[.]org[16] を反転コピーした偽の寄付サイトに切り替えました（図 9 を参照）。このアクターはまた、欧州連合（EU）になりすましたページや、戦争の犠牲者を支援しようとするヨーロッパ人をターゲットにした偽の寄付サイトも作っています。

図 9. supportukrainenow[.]org になりすます偽の寄付サイト

Hasty Hawk は TDS を使用して、ユーザーをさまざまな Web ページに誘導します。これらの Web ページでは、ユーザーの位置情報や場合によっては他のユーザー特性に基づいて、コンテンツと言語を変更しています。ユーザーが使用するデバイス、場所、またはさまざまな時間帯に基づいて異なるコンテンツが表示される場合、バックグラウンドで TDS が動作していることは明らかです。これにより、被害者は犯罪者に最も利益をもたらすページに誘導されます。Hasty Hawk は、ドメインの一部をさまざまなキャンペーンテーマ間で切り替えています。図 10 の例を見てみましょう。これは、FQDN dhl[.]3204[.]thebagshelf[.]com の位置情報に基づくリダイレクトと、時間の経過に伴う Web ページコンテンツの変化を示しています。

16 https://www.globalshapers.org/home

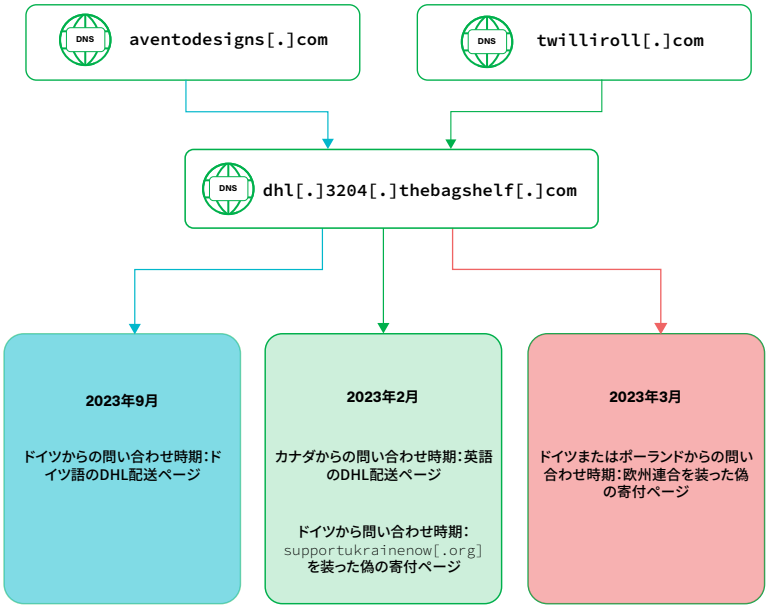

図 *10*：dhl[.]3204[.]thebagshelf[.]com へのリダイレクトの例と、アクターが時間の経過とともに表示した *Web* ページの一部

1. **2023 年 9 月** – FQDN はドイツ語の DHL 配送ページをホストしています。ユーザーは aventodesigns[.]com からそこにリダイレクトされました。[17]
2. **2024 年 2 月** – FQDN は、カナダのユーザー向けの英語の DHL 配送ページ（twilliroll[.]com からリダイレクト）と、ドイツのユーザー向けの supportukrainenow[.]org を偽装している偽の寄付ページの両方をホストしています。
3. **2024 年 3 月** – FQDN は IP を 91[.]212[.]166[.]71 から 91[.]212[.]166[.]14 に切り替え、ドイツとポーランドのユーザー向けに欧州連合を偽装したウクライナへの偽の支援ページをホストしています。

Hasty Hawk は、2024 年を通じてこの単一の FQDN のキャンペーンテーマを変更し続けました。9 月の時点で、この FQDN は、図 11 に示す英語の DHL 配送ページをホストしていたり、ユーザーに「dhl [.]com にアクセスするにはセキュリティチェックを完了してください」と要求する CAPTCHA ページにリダイレクトしたりして、おとりとして正規の DHL Web サイトにリダイレクトしていました。[18]

17 https://urlscan.io/result/520f01c1-c3cf-48ad-9295-95bbd671ea50

18 https://urlscan.io/result/1998c142-5292-4895-98bd-17c04394286b

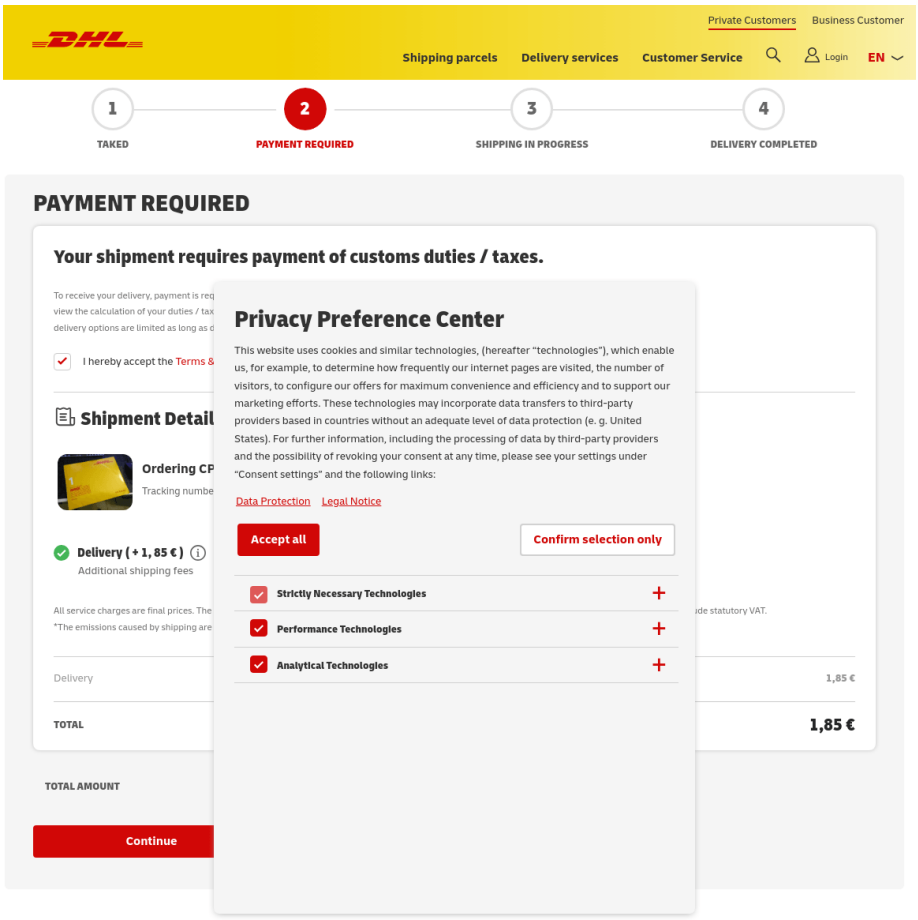

図 *11. 2024* 年 9 月の `dhl[.]3204[.]thebagshelf[.]com` の *DHL* フィッシングページ

VEXTRIO VIPER とアフィリエイト

私たちの調査の結果、Sitting Ducks により乗っ取ったドメインがどんどん発見されるようになりました。2020 年初頭から、一部は VextRio Viper TDS の大規模なインフラストラクチャの一部であることが判明しました。これらのドメインは当初、その古さゆえに目立ちましたが、乗っ取られたことが判明すると、欠けていた部分が見えてきました。本質的には、VexTrio Viper は Vacant Viper と同様の方法で、TDS で乗っ取ったドメインを使用しています。VexTrio は、65 を超えるアフィリエイトパートナーからの侵害された Web トラフィックをルーティングする最大のサイバー犯罪アフィリエイトプログラムを運営しています。そのパートナーのうちのいくつかは、悪意のある活動のために Sitting Ducks 経由でドメインを盗んでもいました。

VexTrio は、かつて DigiCert/DNS Made Easy（DME）、Constellix、DigitalOcean ネームサーバーに委任された正しくない状態のドメインを乗っ取り、TDS サーバーを運用しています。乗っ取ったドメインは、偽の出会いサイトやギフトカード詐欺、偽のロボット CAPTCHA 通知などをホストする下流の悪意のあるコンテンツ発行者や、自社の悪質なサイトにトラフィックをルーティングします。

最も注目すべき例の 1 つは `mpinc[.]com` です。VexTrio が 2023 年 8 月にドメインを乗っ取ったことは確認されていますが、2022 年 4 月には侵害されていた可能性があります。このドメインの元の所有者は、教育研究に重点を置く組織である MPR Associates です。このドメインは、社会、科学、健康問題を専門とする非営利研究機関である RTI International（`rti[.]org`）によって 2013 年に買収されるまで、主に 1990 年代と 2000 年代に活動していました。このドメインは 2015 年後半に DME ネームサーバーに切り替えられました。pDNS によると、`mpinc[.]`

com は 2022 年 1 月から 3 か月間 DigitalOcean IP（157[.]230[.]67[.]179）にパークされていましたが、2022 年 4 月に脅威アクター（おそらく VexTrio）によって乗っ取られました。2023 年 8 月から 10 月まで VexTrio の管理下にあった間、このドメインは、図 12 に示すように、アクターがよく使用する偽の出会い系サイトの 1 つにユーザーをリダイレクトしていました。[19,20] 現在、mpinc[.]com は委任が正しくない状態にあり、権威 DNS サーバーに委任されていません。

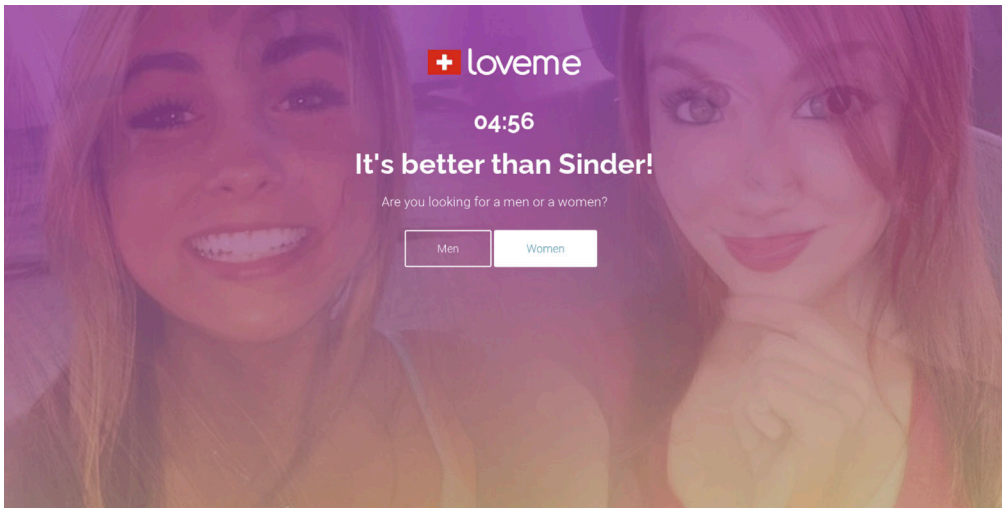

図 12. 乗っ取られたドメイン mpinc[.]com の偽の出会い系 Web ページ

VexTrio は、以前は毎年開催されていた ACM/IEEE 国際サイバーフィジカルシステム会議（ICCPS）で使用されていたドメイン、iccps[.]org も乗っ取りました。このドメインは、2009 年 9 月頃にカーネギーメロン大学の教授によって登録されました。WHOIS 情報によると、このドメインは DME ネームサーバーに委任された後、2023 年 8 月初旬から悪用可能になったと推定されます。その後、VexTrio はこれを TDS インフラストラクチャで使用し、2023 年 9 月から 10 月にかけてユーザーをキャンペーンにルーティングしました。その後、期限切れのドメインに使用された DigitalOcean IP アドレスに解決され、最終的に Bodis IP にパークされ、現在もそこに残っています。ACM/IEEE は現在、会議のために iccps[.]acm[.]org を使用しています。[21] 彼らの会議のために。

VEXTRIO VIPER アフィリエイトが ANTIBOT CLOUD を使用

また、VexTrio Viper のアフィリエイトが Sitting Ducks を悪用しているのも確認しています。そのアフィリエイトの多くは、セキュリティ研究者によるボットやトラフィックをフィルタリングする手段として、ロシアのアンチボットサービスである AntiBot Cloud を使用しています。AntiBot の機能には、IP 位置情報やユーザーエージェントなどの情報に基づいて、特定のボットサービスまたはユーザーをブロックするルールを設定する機能が含まれています。ユーザーは、ボット保護を制限してこのサービスをローカルで無料で実行することも、クラウドプレミアムバージョンにアップグレードすることもできます。表面的には、AntiBot Cloud は本質的に悪意があるようには見えませんが、ユーザーベースの大部分はサイバー犯罪者であるようです。ロシアやその他の東ヨーロッパのサイバー犯罪者に好まれるこのサービスは、もともとロシア語で書かれていましたが、後に英語のコンテンツにも拡張され、ロシアルーブルが主要な支払いオプションの 1 つとして採用されています（図 13 を参照）。AntiBot は、フリーランスのプログラマーとして自ら宣伝している MikFoxi という仮名を持つ 1 人の人物によって完全に管理されているようです。また、AntiBot を使用するのは VexTrio Viper 自体ではなく、アフィリエイトのみであることにも注意してください。AntiBot をブロックしても、VexTrio はブロックされません。AntiBot クラウドサービスの FQDN は次のとおりです。

19 https://urlscan.io/result/7948b668-5226-4670-9b54-63d1da91fee2

20 https://iccps.acm.org/2025/

21 https://urlscan.io/result/8184b40c-2fb1-4036-92bb-3d0942460752/#transactions

- hXXps://antibotcloudapi[.]com/9.php
- antibotcloudapi[.] com
- antibot[.]cloud
- antibotcloud[.]com
- ipv4[.]mikifox[.]com
- ipv6[.]mikifox[.]com
- admin[.]mikifox[.]com

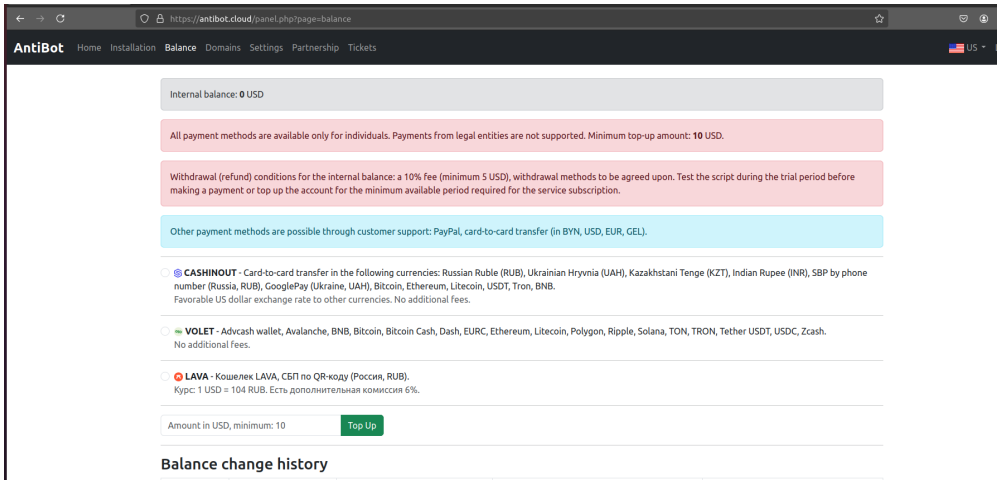

図 *13.AntiBot* の支払いオプション（ロシアルーブルを含む）

AntiBot を使用して missouri[.]com を乗っ取ったあるアフィリエイトは [22] 2022 年 10 月に DME 経由で侵入しましたが、このドメインは以前に他の脅威アクターによって盗まれた可能性があります。そのドメインはこのアフィリエイトによって管理されていましたが、ユーザーは VexTrio Viper が運営する偽の出会い系サイトにリダイレクトされました。最初の乗っ取りの前は、missouri[.]com を使用していた Web サイトは State Ventures, LLC によって開発され、ミズーリ州に関連していた可能性があります。このドメインには以前、ミズーリ州の市や郡専用のサブドメインレコードが多数表示されていました。キャッシュされたデータによると、下の図 14 に示すように、州のビジネスや観光に関連するコンテンツが豊富なサイトでした。さらに、以前のミズーリ州の宝くじサイトは、サブドメイン lottery[.]missouri[.]com に割り当てられていた可能性があります。そのコンテンツは現在、DME ネームサーバーも使用する molottery[.]com でホストされています。

22 https://urlscan.io/result/8184b40c-2fb1-4036-92bb-3d0942460752/#transactions

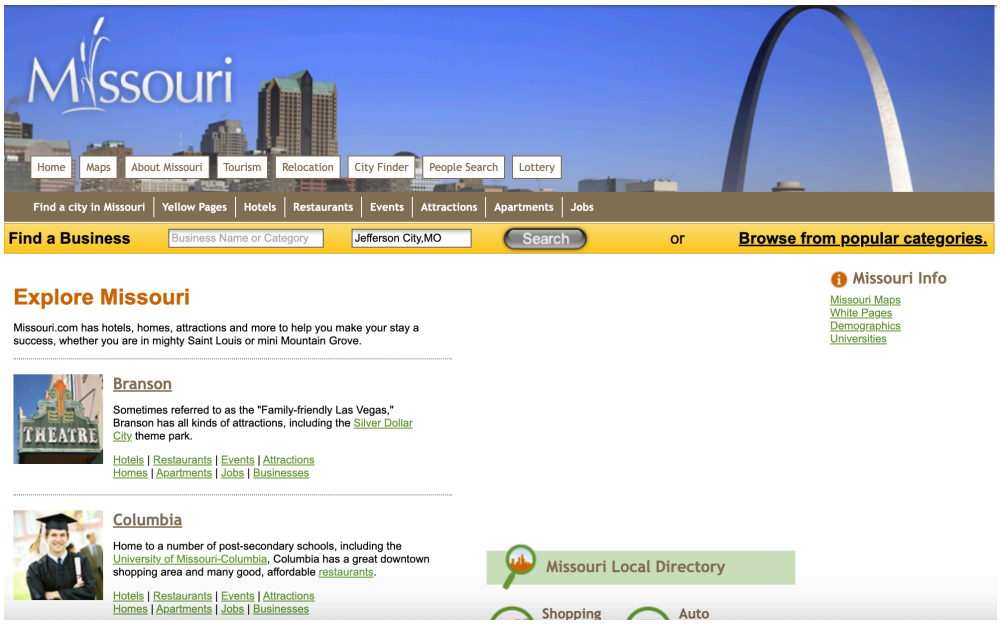

図 *14. 2018* 年 9 月の `missouri[.]com` の *Web* ページ（おそらく乗っ取られる前のミズーリ州の公式ページ）

VEXTRIO GOREFRESH アフィリエイト

GoRefresh は、偽のオンライン医薬品キャンペーンを運営し、オンラインギャンブルや出会い系詐欺などの他のアフィリエイトのキャンペーンに参加する VexTrio Viper アフィリエイトです。GoRefresh は、脆弱な DNS サービスプロバイダーである DME と GoDaddy からドメインを乗っ取りました。このアフィリエイトは、これらの乗っ取ったドメインを使用して、侵害された Web トラフィックを VexTrio や他のアフィリエイト、そして自社の医薬品ランディングページにリダイレクトします。

Vacant Viper と同様に、GoRefresh は通常、HTTP 404 Not Found エラー応答ステータスコードでユーザーに応答します。あるいは、リソースをリダイレクタとして使用する場合、従来の HTTP 302 リダイレクト応答に先立ち、HTML メタリフレッシュによって被害者の Web ページを次の URL に「リフレッシュ」します。この HTML コードリダイレクトの例を次に示します。

```
<meta http-equiv=”refresh” content=”0;http://vipshopevent[.]su”>
```

ローテーションハイジャック

Sitting Ducks の調査中によく見かけたのは、繰り返しての乗っ取りです。1 つのドメインが時間の経過とともに複数のアクターによって乗っ取られています。脅威アクターは、DNS Made Easy のような無料アカウントを提供する悪用可能なサービスプロバイダーを貸出ライブラリとして使用し、通常は 30 ～ 60 日間ドメインを乗っ取ります。しかし、アクターがドメインを長期間保有するケースも見てきました。短期間の無料アカウントの有効期限が切れると、ドメインは最初の脅威アクターによって「紛失」され、その後、別の脅威アクターによってパークされるか、申請されます。

VexTrio Viper のアフィリエイトがこれを頻繁に行っているのを私たちは見てきました。特に、以前 Vacant Viper によって侵害されたドメインを乗っ取る場合によく見られます。例として、下の図 15 に `mcpennsylvania[.]com` の乗っ取りのタイムラインを示します。このドメインは、最初に Vacant Viper によって乗っ取られ、その後 VexTrio Viper のアフィリエイトによって乗っ取られました。WHOIS 情報によると、登録事業者（CSC Digital Brand Services）とネームサーバープロバイダー（DME）は、さまざまな乗っ取りを通じても変更されていませんでした。

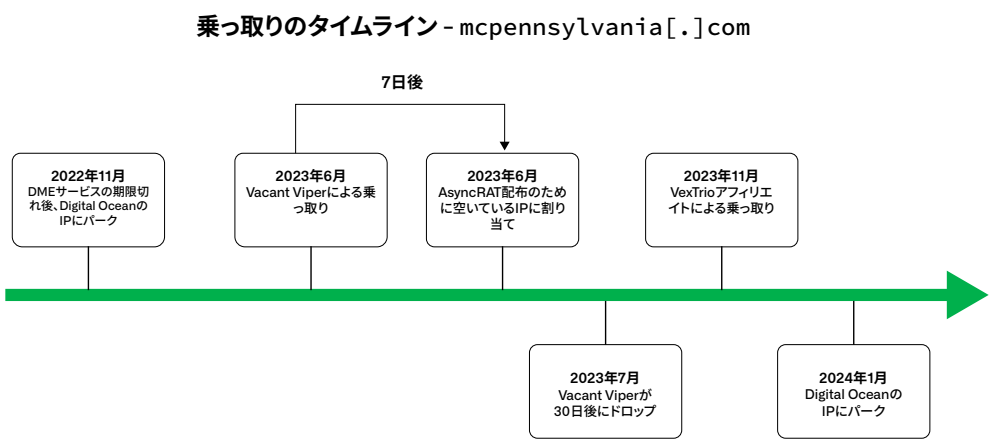

図 15. mcpennsylvania[.]com の乗っ取りのタイムライン

結論

私たちがプロファイルした脅威アクターは、この強力かつ目立たない攻撃ベクトルを利用した人々のほんの一例にすぎません。Sitting Ducks 攻撃ベクトルの影響は広範囲に及びますが、対処が複雑ではあっても完全に予防可能です。アクターは、緩和、そして最終的には防止のための積極的な努力がなされなければ、この攻撃ベクトルを悪用し続けます。情報開示ブログでお伝えしたように、権威ある DNS プロバイダーや登録事業者から政府機関や標準化団体まで、誰もが Sitting Ducks の攻撃を阻止する役割があります。乗っ取りを検出し、できるだけ早く被害を軽減するためのより優れた方法が必要です。正規のドメイン登録者は、登録事業者とプロバイダーの両方がそうであるように、DNS レコードを維持するだけでなく、悪用の報告にも対応する必要があります。

この攻撃は検出が非常に難しいため、脅威アクターが引き続きこの攻撃を利用することは間違いありません。ドメインを乗っ取り長期間保有しているアクターを何人か見つけましたが、その乗っ取りの目的を特定することはできませんでした。これらの乗っ取られるドメインは評判が高い傾向があり、通常はセキュリティベンダーに気付かれないため、巧妙な攻撃者が何の罰も受けずにマルウェアを配信したり、横行する詐欺行為を行ったり、ユーザーの認証情報をフィッシングしたりできる環境が生まれます。できれば、脅威インテリジェンスコミュニティによるこの手法に対する意識が高まるにつれて、アクターの利用が注目され、乗っ取られたドメインの追跡と修復が可能になることを願っています。

Infoblox 製品は Sitting Ducks に対して脆弱ではありませんが、お客様が登録するドメインの DNS の運用方法によっては影響を受ける可能性があります。したがって、すべてのドメイン名所有者、特にサードパーティの DNS システムを使用していてそのサービスステータスを認識していない所有者は、図 16 の 3 つの質問に従ってリスクレベルを評価することをお勧めします。

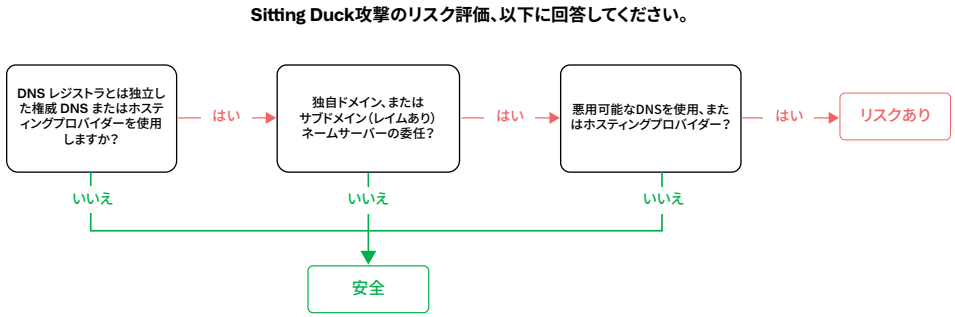

図 16. *Sitting Ducks* 攻撃のリスクがあるかどうかを判断するための 3 つの質問

SITTING DUCKS の犠牲者

このレポートで説明した乗っ取られたドメインは、さまざまな業界の正当な組織に属していました。ドメインは、その存続期間中に複数の異なる所有者を持つことができます。以下のリストには、ドメインが乗っ取られる前に特定した正当な所有者が含まれています。

乗っ取られたドメイン	正当なドメイン所有者
agbizwichita[.]org	Agri-Business Council of Wichita
alonbyacarian[.]com	Acarian Systems Alon Capri Loudspeakers
aphecalenterprises[.]com	Aphecal Enterprises Inc.
clickermediacorp[.]com	CBS Interactive
iccps[.]org	International Conference on Cyber-Physical Systems
jmnet[.]com	JM Eagle
mbhs[.]com	MISSISSIPPI BAPTIST HEALTH SYSTEMS, INC.
mcpennsylvania[.]com	McDonald's Corporation
missouri[.]com	State Ventures, LLC およびおそらくミズーリ州
mosaicmedicalsupply[.]com	Mosaic Medical Supplies（整形外科用・化粧品卸売業者）
mpinc[.]com	MPR Associates（法律事務所）
mstouchenaturals[.]com	MS TOUCHE
mygemcon[.]com	Gemcon Group
ncbtv[.]com	NCBTV（IPTV サービスプロバイダー）
successbusinesspages[.]com	Success Business Pages（オンラインビジネス・ディレクトリ）
thebagshelf[.]com	Thai online apparel store
tmsec[.]com	T&M USA（民間警備・調査会社）
uni-t[.]com	Bridgestone - Firestone Tire Sales Company

アクティビティの指標

以下の表は、これらの脅威アクターが使用したアクティビティ指標（IOA）を示しています。詳細については、Infoblox Threat Intelligence GitHub リポジトリ（https://github.com/infobloxopen/threat-intelligence/tree/main）を参照してください。

指標	タイプ	注記
oil-poland[.]site balticpipe[.]playroom8[.]site	ドメイン	Horrid Hawk が登録し、キャンペーンで使用した類似ドメイン
mstouchenaturals[.]com covidianmuseum[.]com alhej[.]com agbizwichita[.]org aphecalenterprises[.]com	ドメイン	Horrid Hawk キャンペーンで使用された乗っ取られたドメイン
thebagshelf[.]com successbusinesspages[.]com aventodesigns[.]com twilliroll[.]com	ドメイン	Hasty Hawk キャンペーンで使用された乗っ取られたドメイン
aerospaceavenue[.]com affixio[.]com adventsales[.]co[.]uk afarm[.]net affiliatebash[.] comamikamobile[.] comafcmanager[.]net adztrk[.]com clickermediacorp[.]com mcpennsylvania[.]com	ドメイン	Vacant Viper キャンペーンで使用された乗っ取られたドメイン
mpinc[.]com iccps[.]org jmnet[.]com ncbtv[.]com uni-t[.]com tmsec[.]com mbhs[.]com	ドメイン	VexTrio Viper キャンペーンで使用された乗っ取られたドメイン

指標	タイプ	注記
missouri[.]com mcpennsylvania[.]com	ドメイン	AntiBot Cloud アフィリエイトキャンペーンで使用された乗っ取られたドメイン
mosaicmedicalsupply[.]com	ドメイン	VexTrio GoRefresh アフィリエイトが使用した乗っ取られたドメイン
vipshopevent[.]su	ドメイン	VexTrio GoRefresh 製薬キャンペーンで使用されたドメイン
alonbyacarian[.]com fixedsights[.].com mygemcon[.]com sauda-pati[.]com tewksenterprises[.]com ummatie[.]com xiangmanlou[.]com	ドメイン	健康詐欺のアクターが使用した乗っ取られたドメイン
hXXps://ecole-artcom[.]com/wdown/ hXXps://www[.]mediasimulasi[.]com/wazxd	URL	AsyncRAT ダウンロードに関連付けられた URL
https://wercosliuhqgheirn[.]com/ hXXps://moarhofhechtl[.]at/wp-content/plugins/image-hover-effects-addon-for-elementor/download[.]php	URL	DarkGate のダウンロードに関連付けられた URL
hXXps://antibotcloudapi[.]com/9.php antibotcloudapi[.]com antibot[.]cloud antibotcloud[.]com ipv4[.]mikifox[.]com ipv6[.]mikifox[.]com admin[.]mikifox[.]com	FQDN	AntiBot クラウドサービスで使用された FQDN

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 : 20241030v1