infoblox®

LOOKAL1KE DOMAIN 攻撃の深層に迫る

新しい調査で最新の攻撃方法が明らかに

2023 年 4 月

LOOKALIKE DOMAIN はすべての人がターゲット

目次

エグゼクティブサマリー

インターネットの出現以来、脅威アクターは、パッと見て類似したドメインを使用して、ユーザーを悪意のある Web サイトに誘導させてきました。これらのドメインはLookalike domain（類似ドメイン）と呼ばれ、フィッシング攻撃と同義であるため、セキュリティ意識向上トレーニングには、フィッシング攻撃のリンクを検査する方法の学習も含まれています。

しかし、意識向上キャンペーンやテクノロジーの進歩にもかかわらず、類似ドメインは消費者や組織にとって絶えざる脅威であり、攻撃者は継続的に使用し続けています。誰もがターゲットです。消費者から政府まで、大手小売ブランドから町のレストランまで、世界的に有名なテクノロジー企業から知名度の低い企業まで狙われています。このレポートでは、実際のドメインと組織的活動の例を示して「誰もがターゲットである」ことを説明していきます。かなりニッチな業界でそれなりの規模の企業である私たちでさえ、標的にされるのです。

このレポートでは、業界やユーザーグループ全体の実例を紹介することで、現在の脅威の状況を説明しています。Infoblox は、長年にわたって類似ドメインを検出しており、毎日 700 億を超えるドメインネームシステム（DNS）イベントを分析して、新しい潜在的な脅威を発見しています。このレポートでは、2022 年 1 月から 2023 年 3 月までの検出に焦点を当てました。300,000 を超える 類似ドメインから、これらの攻撃に関連する課題とリスクに焦点を当てた例を集め説明しています。

類似ドメインは、メールスパム、広告、ソーシャルメディア、SMS などを介して、消費者をターゲットとしない広範な攻撃と関連付けられることがよくあります。毎日何千もの一般的なソフトウェア、金融機関、宅配サービスを模倣したドメインが新規に登録されています。ユーザーの認証情報を盗んだり、コンピュータをマルウェアに感染させたりすることを目的としたフィッシング攻撃は広く蔓延しており、多くの場合、あまりに洗練されていないため、「メールをチェックしなければフィッシング詐欺に引っかからない」など、数多くのミームの元になっています。フィッシングはコミカルなイメージが強いと思われがちですが、フィッシング業界は、とても真剣に取り組んでいます。Anti-Phishing Working Group (APWG: フィッシング対策協議会) は、フィッシングが 2022 年第 3 四半期に記録的なレベルに達したと報告しています。[1]

[ ] **このレポートに記載されているすべての類似ドメインと思われるものは、悪意があるか正当であるかに関係なく、無効化されています。ピリオドを括弧 *[.]* で囲んで類似ドメインを無効化し、クリック可能なリンクにならないようにしています。**

700+ 億

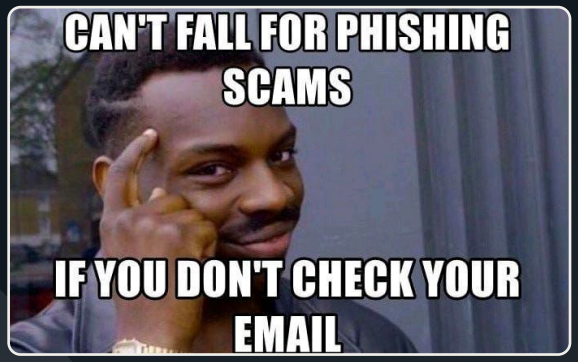
Infoblox は、毎日 700 億件を超える DNS イベントを分析して、新たな脅威を特定しています。

30 万 +

このレポートでは、これらの攻撃の課題とリスクを強調するために、類似ドメインを公開しています。

フィッシングミームの一例

その一例は、2019 年のこのツイートです。[2]



画像著作権 : このミームの出所は不明です。

しかし、類似ドメインは消費者にとって脅威であるだけではなく、企業ネットワークにアクセスするためにも使用されています。

最近の情報公開により、悪意のあるアクターが従業員をだまして多要素認証 (MFA) 情報を提供させる標的型攻撃が明らかになりました。ほとんどの場合、類似ドメインは会社を模倣するだけでなく、MFA キーワードも含まれており、接続が安全であるかのように従業員に錯覚を起こさせるように強化されています。世界中のインターネットサービスプロバイダー、銀行と暗号通貨、ソフトウェアとサービス、保険会社を含む、多くの業種にわたり世界中の大小の企業が攻撃アクターによって標的にされていることが判明しました。これらの攻撃は 2022 年初頭に始まり、時間の経過とともに勢いを増しました。

類似ドメインの使用は、非対称な攻撃であるため、利益になります。ユーザーは、自分の資産や雇用主の情報を保護するために常に警戒する必要があります。ドメイン登録価格が安く、大規模に攻撃を分散させることができるため、攻撃者は優位に立つことができます。攻撃者には規模という利点があり、悪意のある活動を特定する技術は長年にわたって改善されていますが、防御側は攻撃アクターのペースに追いつくのに苦労しています。

類似フィッシングが蔓延しているだけでなく、類似フィッシングの使用はより複雑になっており、その方法は DNS レコードで最も顕著になっています。当社の調査では、類似ドメインが従来のフィッシングやタイポスクワッティングの目的を超えて活用されていることが示されています。これらは、ネームサーバーとしてやスピアフィッシング (標的型フィッシング) メールの配布など、これまで報告されていない方法でも使用されています。類似ドメインのみをサービスし、消費者と政府職員の両方を標的とする、回復力のある大規模なネットワークが存在します。

Infoblox には、類似ドメインを識別するための複数のアルゴリズムがあります。当社は、ショッピング、バンキング、ソフトウェア、金融部門で一般的なターゲットの亜種の監視、顧客が指定したドメインの亜種の監視、類似ドメインを専門とする DNS インフラストラクチャの攻撃アクターの監視など、様々な方法を組み合わせています。この多面的なアプローチにより、脅威の状況を幅広く網羅できるようになります。

重要: このレポートには、実際に存在する類似ドメインの広さと深さを示す多数の例が含まれています。これらは、何らかの組織に対する攻撃や侵害の成功を示唆するものではありません。

背景

他の優れた研究論文と同じように、まずはいくつかの背景情報から説明を開始していきます。これは主に用語についてです。ほとんどの読者が背景セクションを読まないか、飛ばし読みすることはわかっていますので、短くしておきます。

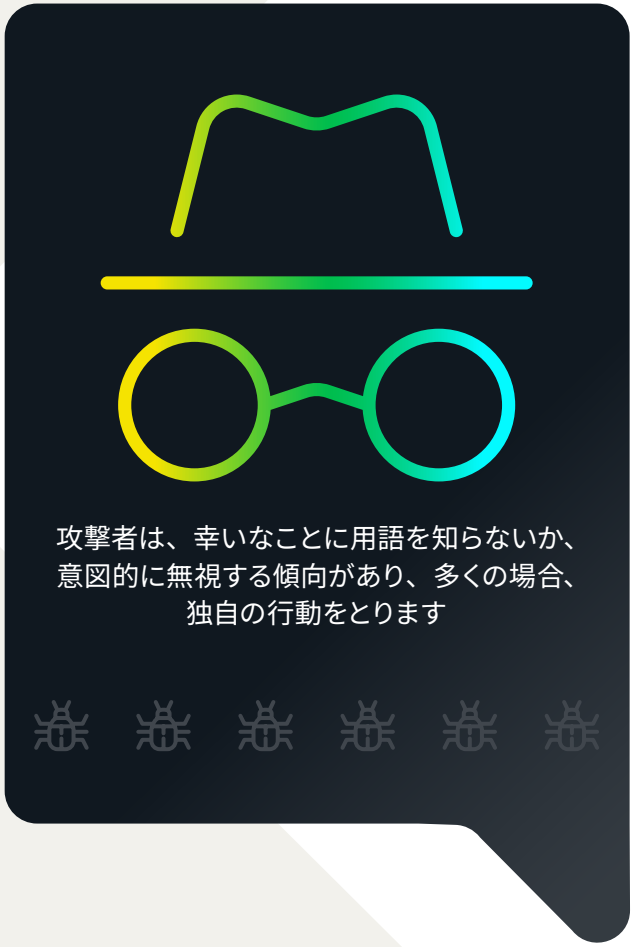
悪意のある類似ドメイン (既知のドメインと同じまたはよく似たドメインを登録して攻撃) は、サイバー環境においてよく知られた、絶えることのない脅威です。一般的に言うと、類似ドメインには攻撃的な用途と防御的な用途の両方があります。攻撃的という意味では、人間の目の届くところならどこでも、類似ドメインは、騙すために使われます。攻撃アクターは、類似ドメインを使用して、金銭を盗んだり、認証情報やアクセス権を取得したり、個人を特定できる情報を収集したり、マルウェアを配布したり、広告収入を得たりします。また、政治的な目的やブランドの評判を傷つけるためにも使用されます。つまり、サイバー犯罪者にとっては目的を達成するための手段なのです。防御の意味では、多くの組織は、攻撃者がそのドメインを主張して使用することを防ぐために、自社のドメインと同様のドメインを積極的に登録しています。

類似ドメインには様々な形態があります。DNS 空間では、ドメインは次のように分けられます。

- **ホモグラフ**
- **タイポスクワット**
- **コンボスクワット**
- **サウンドスクワット**

それらは、元の標的ドメインとほとんど区別がつかない場合もあれば、客観的にまったく区別できない場合もあります。攻撃方法としての類似ドメインの成功の多くは、各個人の責任によるものです。

これから説明するように、メール送信者のアドレスからフィッシング URL、マルウェアコマンドアンドコントロール (C2) に至るまで、攻撃のあらゆる要素で類似ドメインが見つかる可能性があります。通常はアドレスレコード (A/AAAA) に関連付けられていますが、ネームサーバー (NS)、ポインター (PTR)、正規名 (CNAME) レコードに使用される類似ドメインも見つかりました。それらは、メール、SMS または SNS、侵害された Web サイト、マルバタイジング (悪意のある広告) ネットワーク、電話を通じて展開される可能性があります。次のセクションでは、類似ドメインの様々な形態について簡単に説明し、それぞれの例を示します。



タイプライターのせいにする

実は、この現代的な問題は、タイプライターの時代の初期にまでさかのぼることができます。多くの古いタイプライターには 0 や 1 のキーがなく、タイピストは大文字の O や小文字の L を使ってこれらの数字を表すことになっていました。[4]

ホモグラフ

英語のホモグラフ (homograph) は、「同じスペルの 2 つの言葉であっても同じ発音にならず異なる意味をもつ、同音異義語」という意味で、ホモグラフという言葉は、長年にわたりセキュリティ研究の文献で使用され、「視覚的に同じに見える 2 つのドメイン」を意味しています。[3] もっと正確な単語はホモグリフ (homoglyph) です。これらのドメインはそれぞれとてもよく似ていて、ほぼ識別がつかない場合もあります。調査文献との一貫性のために、このレポートでは不正確な単語である、ホモグラフを使用します。

この類似ドメインの形態は、同じ文字の並びまたはアルファベット内の多くの文字が互いに似ていることをうまく利用しています。たとえば、0 (数字のゼロ) と O (大文字の「o」) または「l」(小文字の「L」) と「I」(大文字の「i」) です。フォントによっては、この問題をさらに悪化させるものもあります。この典型的な例は g0ogle.com と Infoblox.com で、Google の綴りの「o」をゼロ (0) に、Infoblox の「i」が小文字の「L」に置き換えられています。

インターネットが成熟し、英語を母国語としない人々が World Wide Web (ワールドワイドウェブ) にログオンし始めて、国際化ドメイン名 (IDN) の必要性が高まりました。IDN は、非ラテン文字を少なくとも 1 つ含むドメインです。ユニコードの導入により、そのようなドメインの台頭が可能になりました。IDN には、IDN ホモグラフという新しい形の類似語が登場しました。これはまだ homograph ですが、他の文字の並びや類似したアルファベットの文字を使用するものです。Gabrilovich と Gontmakher は、2002 年の論文「The Homograph Attack (ホモグラフの攻撃) 」で IDN homographs の力を示しました。著者は、キリル文字の「c」と「o」を含めた、本物の Microsoft ドメイン microsoft[.]com に類似したドメインを登録していました。[5] 最終的な結果は、ドメイン www.microsoft[.]com は、本物の Microsoft ドメインと視覚的に区別がつきません。

ユニコード協会は、特定の文字列に使用できる膨大な数の紛らわしい文字を示すツールを公開しました。[6]「hi」の文字列にはユニコード文字を含む 684 のバリエーションがあり、「infoblox」のような文字列の場合、そのバリエーション数は 2.2 兆を超えるまでに膨れ上がります。一部のバリエーションは、他のバリエーションに比べて、類似性の効果が低くなります。たとえば、ユニコード協会は、「٥」(アラビア・インド数字の 5 桁) を「o」(アルファベットの「O」の小文字) と混同しやすい文字として挙げています。

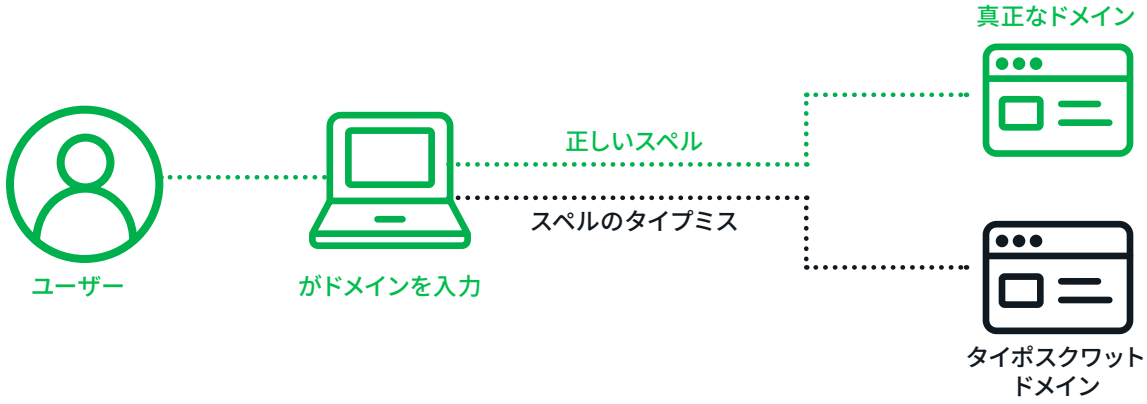
明らかに、*inf٥bl٥x[.]com* はあまり類似という効果はありませんが、一般的に使用される *Arial* フォントで表示された場合、正しいドメイン *{infoblox[.]com} and {infoblox[.]com}*(ベラルーシ語またはウクライナ語の小文字「*i*」とアルメニア語の小文字「*vo*」は「*n*」と書かれる) を区別することができますか？私たちでも区別できません。

タイポスクワット

タイポスクワットドメインは、人気のあるドメイン名と、ユーザーが犯す、または壊れたキーボードでの入力によって引き起こされる入力ミスを利用します。この用語は通常、広告収入を得るために登録されたものの未使用のままになっているドメインに関係しています。例えば、著者の 1 人は最近、appfolio[.]com (不動産管理グループや家主に SaaS ソリューションを提供する有名なソフトウェア会社) でホストされている不動産管理グループのオンラインポータル経由で家賃を支払おうとしていて、誤って、appfollio[.]com にアクセスしそうになりました。そのドメインは、2013 年に登録され、現在は停止状態です。

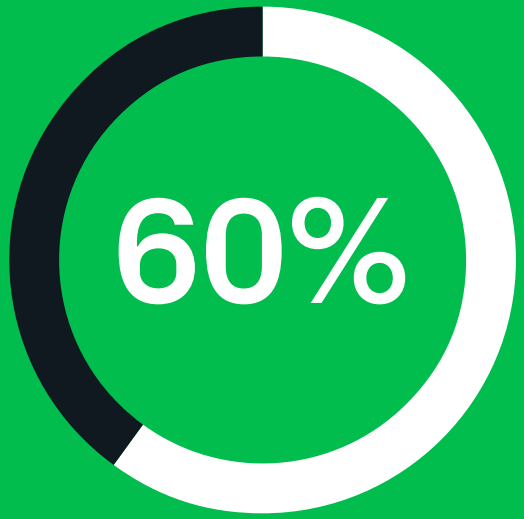
興味深いことに、Appfolio のもう 1 つの明らかなタイポスクワットドメインである apfolio[.]com は、Appfolio が所有しているようです。このドメインは適切なドメインにリダイレクトされ、同じ登録者、登録組織、登録機関であり、正規のドメイン appfolio[.]com からわずか 1 か月後に登録されました。これは、類似ドメインの防御的な使用例です。残念ながら、組織がすべての類似バリエーションを登録するには可能性のあるバリエーションがあまりにも多すぎるため、悪意のあるアクターが優位に立っています。

タイポスクワットは主に収益化の手段として見られていますが、邪悪な目的を持っている場合もあります。これらは、サードパーティの広告を販売したり、正規のドメイン所有者に販売したりするために使用される一方で、後で説明するように「ブラックハット」アフィリエイトマーケティングプログラムやマルウェア C2 ドメインとしても使用される可能性があります。ブランドや企業は、反サイバースクワッティング消費者保護法に基づいて、タイポスクワッティングに対して保護を受けられます。この法的措置の脅威のために、タイポスクワッティングはドメインフリッピング (ドメインの転売) / ドメインパーキングのコミュニティでは収益化の「ブラックハット」な形態とみなされており、iGoldrush のような真面目なドメインフリッパーは、利益を得るためのタイポスクワッティングを推奨していません。[7]



タイポスクワットの例

gikthub[.]com
5whatsapp[.]com
Hdfcbank[.]vip
royalbsank[.]com
sportybet[.]city
bamgkokbank[.]com
1337x[.]asia
moneycont5rol[.]com



悪用されたコンボスクワッティングドメイン

悪用されたコンボスクワッティングドメイン最初の解決から 100 日後に少なくとも 1 つの公開ブロックリストに掲載される

コンボスクワッティング

コンボスクワッティングは、人気のブランド名や企業名と他のキーワードを組み合わせた Lookalike domain 攻撃の形態です。サポート、ヘルプ、セキュリティ、メールなどの用語が一般的です。例えば、wordpresssupport[.]ru、wordpresssupport[.]store、wordpress-security[.]cloud を考えてみましょう。これらのドメインはすべて、同じロシアベースの IP アドレスでホストされていて、人気のある Web コンテンツソフトウェアである WordPress に似ています。ドメイン名にサポートとセキュリティが含まれていて、これらが WordPress ユーザーを対象としていることを示しています。これらは、WordPress サイトをハイジャックするための認証情報を収集したり、支払いや個人識別情報 (PII) の詳細を収集したりするために使用される可能性があります。

攻撃アクターは、コンボスクワットドメイン自体を生成するだけでなく、辞書ドメイン生成アルゴリズム (DDGA) を使用して類似ドメインを作成することもできます。数秒で、多数のブランドや企業の数千のドメイン候補を生成できます。純然たる運により、アルゴリズムは、ドメインを効果的にするための適切なキーワードを含むドメイン候補を作成できます。大人気のゲームプラットフォームである Steam のユーザーコミュニティは、コンボスクワット DDGA を使用する攻撃アクターにとって一般的なターゲットです。最近観察されたセット内のドメインの例としては、steamcommiunity[.]com[.]ru、steamcommunity[.]com[.]ru、steamcommunityjp[.]top、steamcommunityiq[.]top があります。このドメインセットでは、タイポスクワッティングとコンボスクワッティングの両方が使用されていることに注意してください。

Kitsin らは、2017 年にコンボススクワッティングの長期的研究を実施し、約 4,680 億件の DNS レコード (稼働中のデータセットと稼働していないデータセットの両方から取得) を分析し、次のような気がかりな結果を発見しました。

- **コンボスクワッティングドメインは、タイポスクワットドメインよりも 100 倍以上普及**
- **不正なコンボスクワッティングドメインの 60% は 1,000 日以上活動**
- **コンボススクワッティングを悪用するドメインの 20% が、最初の解決から 100 日後に少なくとも 1 つの公開ブロックリストに掲載**
- **コンボスクワッティングドメインの解決が前年比で増加 [8]**

コンボスクワッティングドメインの普及に関する著者の見解に当社は同意します。当社の分析でも、純粋なタイポスクワットや純粋なホモグラフ (*IDN* またはその他) よりも、コンボスクワットドメインの方を多く見つけています。

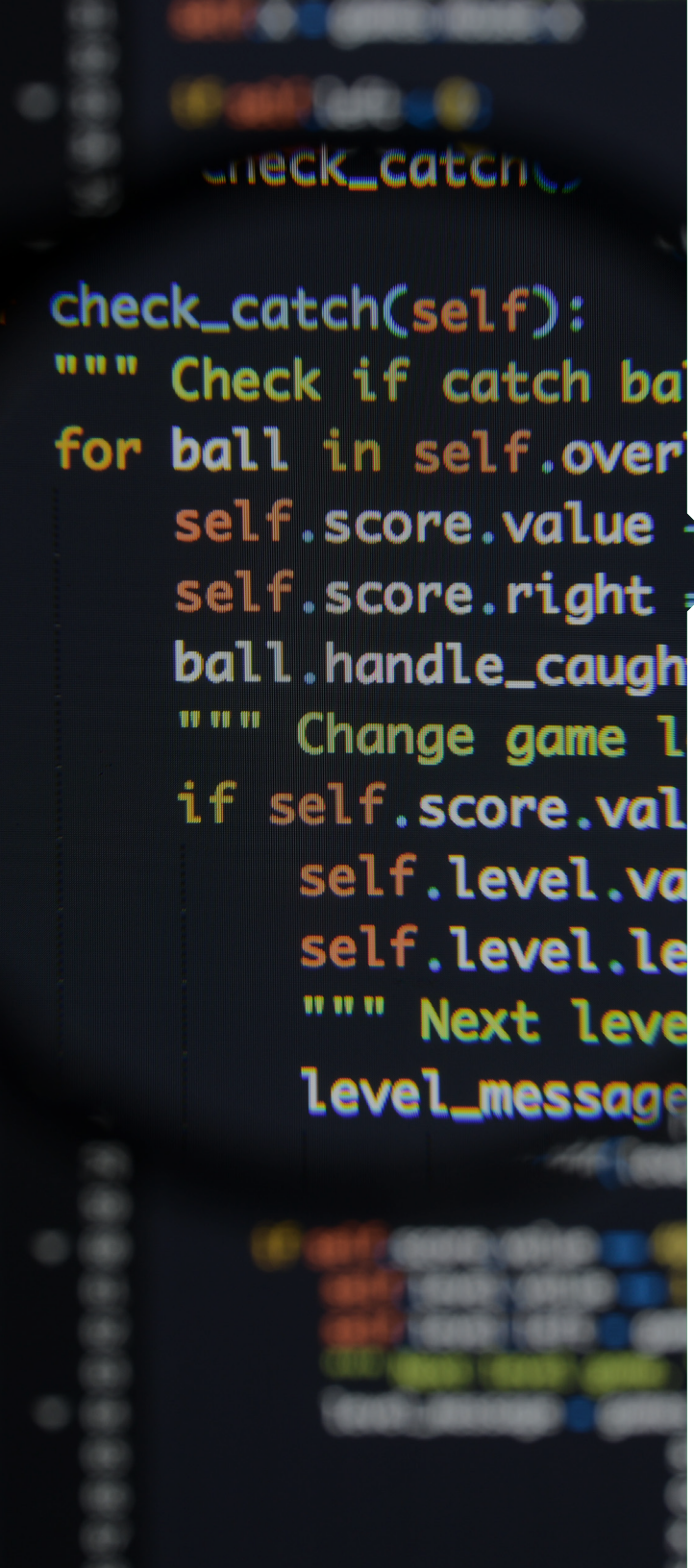
サウンドスクワッティング

サウンドスクワットドメインは、同音異義語、つまり同じ発音でスペルが異なる単語を利用します。サウンドスクワッティングは、2014 年に初めて文献に登場した、最も最近確認された類似ドメインの形態です。[9] サウンドスクワッティングは、Alexa、Siri、Google Voice などのスマートスピーカーの普及により、最近、研究者の注目を集めるようになっています。[10] サウンドスクワットドメインは、他の類似ドメインタイプと重複して使用され、音も見た目も似ている可能性があります。私たちは、純粋なサウンドスクワッティングドメイン、つまり視覚的には似ていないが、音が似ているドメインはまれであることを発見しました。一般的に、これらのドメインは、テキストベースの類似性技術によっても見つけることができます。

実際の世界での類似は、ここで説明したようなきちんとした引き出しに収まらないことが多いことに注意する必要があります。形態の組み合わせは、類似ドメインの効果を最大化するために使用されます。当社が目にするコンボスクワットドメインの多くは、タイポスクワットとホモグラフ（IDN またはその他）の要素を持っています。タイポスクワットはホモグラフの要素を利用し、サウンドスクワットはタイポスクワットの要素を利用します。その結果、攻撃者は防御者を息切れさせることになります。

サウンド攻撃

Alexa、Siri、Google Voice などの音声起動テクノロジーの出現により、サウンドスクワッティングの普及が始まりました。



他の形態の類似ドメイン

このレポートの焦点は、類似ドメインと現在の脅威状況におけるその役割についてですが、脆弱なユーザーを悪用できる他のタイプの類似ドメインも存在します。それらのうちの注目すべき 1 つの例が、最近 Python PyPi パッケージで見つかりました。

https://infosec.exchange/@tweedge@cybersecurity.theater/109846797159938702

Python などの一般的なプログラミング言語のパッケージマネージャーには、ドメインと同じ弱点があります。誰でも、セキュリティリスクがあるかもしれないし、またはないかもしれない不明なコードを含む任意の名前 (同じ名前が使用されていない限り) でパッケージをアップロードできます。2016 年に、セキュリティ研究者の Nikolai Tschacher 氏は、この方法でタイポスクワッティングを採用し、17,000 以上の異なるホストに任意のコードを実行させました。[11] その後、2021 年にセキュリティ研究者の Alex Birsan 氏が Tschacher 氏の考えを発展させ、「依存関係のかく乱」という用語を作り出しました。[12]

Birsan 氏は、様々なオープンソースを通じて、大手企業の非公開の社内パッケージ名を発見しました。これには、Web サイトでソースコードを探索したり、GitHub でパッケージを探したり、公開フォーラムでパッケージ名を検索したりすることも含まれます。次に、プライベートの内部パッケージと同じ名前のパッケージを公開されているパッケージマネージャーにアップロードしました。最後に、Birsan 氏は自動化された CI/CD パイプラインを利用し、公開されているパッケージをプライベートな内部パッケージと「かき混ぜる」ようにしました。自動化されたパイプラインは、プライベートパッケージをインポートしてインストールするのではなく、代わりに Birsan 氏の公開しているパッケージを見つけてインポートしました。その後、Birsan 氏は DNS 抽出を使用して、意図したプライベートパッケージではなく、任意のコードが実行されたことを自分に通知するように設定しました。Birsan 氏の類似技術により、パッケージをアップロードしてから数時間以内に 35 の組織へ侵入できました。

類似ドメインの種類や使用される専門領域に関係なく、類似ドメインは継続的な脅威の一つです。類似ドメインを研究する際の課題の 1 つは、それらが定義されていないことです。つまり、計算できる以上の可能性があり、すべてが対象となります。次のセクションでは、ターゲット、展開方法、インフラストラクチャ、それらが効果的である理由、課題、問題に対する Infoblox の解決策など、実際に存在するさまざまな形態の類似ドメインの具体例を紹介していきます。

誰もがターゲット

この例では、少なくとも１つの驚くべきターゲットが見つかると思います。

DNS の類似ドメインの検査で得られた最も強力な発見の１つは、誰もがターゲットであるということでした。予想されるすべてのターゲットだけでなく、小規模な企業やサービスの類似ドメインも見つかりました。これらのドメインは、職場や家庭で個人を狙って、悪意のあるアクターによって使用されます。

Akamai が最近指摘したように、ほとんどの類似ドメインの組織的活動は、大規模なターゲットに影響が及んで初めて報道されます。[13] 当社の目的はこれらの「典型的な」標的と並んで、報告があまりされない、または見落とされている標的に光を当てることです。ここでは、この点を示すためにいくつかの例を紹介しますが、様々な業界への影響について、そして様々な方法論の使用については、後で詳しく説明します。

当社が標的にされています！

Infoblox は中規模の会社で全世界での従業員数は 2,000 人未満です。

当社は、DNS、Dynamic Host Configuration Protocol (DHCP)、IP アドレス管理 (IPAM) 市場 (総称して DDI として知られます) で大きなシェアを占めていますが、この業界はかなり特殊であり、Infoblox は一般消費者にはなじみのない名前です。悪意のあるアクターが当社のことを認識しており、ましてや、類似ドメインで当社を積極的にターゲットにしていることに驚く人もいるかもしれません。それにもかかわらず、従業員と顧客の両方を騙すように設計されたドメインを多数見つけました。当社の福利厚生ポータルを含む内部サービス、また、当社の製品名などが過去 1 年間に登録されています。

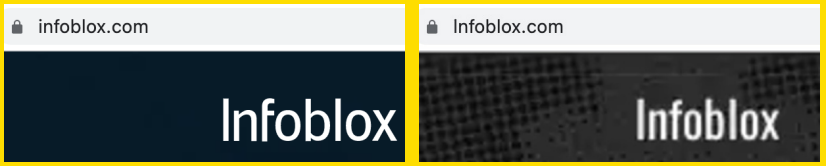


図 2. infoblox[.]com **公式サイト (左) と** Infoblox[.]com **偽サイト (右) のロゴの比較。**

Infoblox が所有していない登録済みドメインには次のようなものがあります。

ホモグラフ **Infoblox[.]com**	小文字の「L」を使って大文字の「I」に代えて、2022年7月に登録され、販売されていますが、サイトの左上隅には当社のコーポレートサイトとほとんど見分けがつかないレンダリングが表示されています。図 2 の比較をご覧ください。
タイポスクワット **infobloxbenifits[.]com**	このドメインは 2022 年 4 月に中国で登録されたもので、従業員福利厚生ポータルからの当社の従業員によるちょっとしたタイプミスです。このドメインは現在、Bodis で保管されています。
TLD (トップレベルドメイン) スクワット **infoblox[.]info**	2022 年 8 月に、悪用の多い登録サイトの Sav[.]com を通じて、別のトップレベルドメイン (TLD) が登録されました。 これは dan[.]com に保管されており、ユーザーはドメインを販売できます。
コンボスクワット **infobloxgrid[.]com**	コンボスクワットは、世界中の何千ものお客様が使用している当社の主力オンプレミス製品によく似ています。当社の特許取得済みの Grid™ technology により、ネットワーク管理者は様々なネットワークアプリケーションを単一のシステムに結合できます。このドメインは dan[.]com でも利用でき、2022 年 4 月に登録されました。
コンボスクワット **infoblox-updater[.]com**	「アップデート」や「サポート」など、ドメイン内で一般的なソフトウェア用語を使用する手法の例。この例では、お客様は、Infoblox のシステムアップデートに関連していると思い込んで、偽のシステムに接続するように誘導される可能性があります。このタイプのコンボスクワットドメインは、テクノロジー企業の名前や製品が頻繁に利用され、フィッシングドメインやマルウェア C2 として使用される可能性があります。その他の例としては、dev[.]gitlabs[.]me と jira[.] atlas-sian[.]net があり、いずれも Advanced Persistent Threat (APT) 攻撃の Iron Tiger が SysUpdate マルウェアで使用されています。[14]

当社のような小規模テクノロジー企業をターゲットにすることに加えて、レストラン、法律事務所、その他の中小企業を語る類似ドメインを広範囲に確認してきました。

さらに、単一の攻撃アクターが、誘い込みとして有名ブランドと中小企業の両方を使うこともあります。Infoblox がしばらくの間追跡してきたある攻撃アクターは、ニューヨークのレストラン Cotenna に類似したドメインを作成し、レストランの Web サイトをコピーし、サイトの訪問者にクレジットカードを使用してオンラインでの予約をするように誘導することを目的としていたようです。[15] cotenna[.]nyc は 2022 年 4 月に登録され、レストランの Web サイト cotenna[.]com の類似ドメインです。この同じ攻撃アクターは、Twitter のような大規模なソーシャルメディア企業を標的にした類似ドメインを持っています。

次のセクションでは、現在最も広く標的にされている業界と、攻撃を成功させるためにドメインを使用する様々な方法のいくつかについて詳しく説明します。誰もが標的となるため、300,000 の類似ドメインの検査に基づいて、最も悪意のある活動が確認された領域を中心に紹介していきます。

LOOKALIKE DOMAIN 攻撃はだれかれ構わず狙ってくる

amėricafirst[.]com
ınstagram[.]dev,
caterpillarespaña[.]com
steamcommunltly.net[.]ru
boatairbuds[.]in
secure1-scotiabank[.]com
saveukraine[.]xyz
expressvpn-app[.]com

10,000+ 組織

2022 年 7 月、Microsoft は、ユーザーからリアルタイムで MFA 認証情報を盗むことを目的とした AitM 攻撃の標的となっている組織が 10,000 を超えていると警告を発しました。

1,600+

当社の調査では、1,600 を超えるドメインに企業機能と MFA と類似する機能の組み合わせが含まれていることを発見しました。

従業員がターゲット

最近まで、多くの企業は、多要素認証 (MFA) を使用して、内部ネットワークをフィッシング攻撃から保護しようと考えていました。

しかし 2023 年初頭、Coinbase は、同社の従業員が社内の MFA ログインに類似のドメインを使用したスピアフィッシング攻撃の標的にされていたことを発表しました。
この発表の直後に、同様の攻撃の標的となった他の企業からの裏付け報告が相次ぎました。被害者からの報告に基づいて、悪意のあるアクターが従業員にメールだけでなく SMS メッセージを送信し、内部システムへのサインインを促したことがわかっています。一部のケースでは電話での連絡もあり、その際に攻撃者は従業員が Web ブラウザでアクセスできるようにドメイン名を提供していました。攻撃者は、中間者攻撃 (AitM) 技術を使用し、従業員が会社の実際のネットワークと対話していることで安心させていました。従業員は MFA コードの入力を求められ、そのコードが攻撃者によって盗まれ、内部システムへのアクセスに使用されました。

Microsoft は 2022 年 7 月に、1 万を超える組織がリアルタイムでユーザーから MFA 認証情報を盗むように設計された AitM 攻撃の標的になっていると警告していました。[16] これらの攻撃は Outlook 365 認証の使用に特化したものでしたが、Microsoft はさらに 2023 年 2 月に、MFA 攻撃を可能にするフィッシングキットが 2022 年 7 月に販売され、広く使用されていると報告していました。[17] Twilio を含む他の企業も 2022 年夏に同様の攻撃を公表していましたが、Coinbase の発表まで攻撃の広範さはあまり公表されていませんでした。[18]

このインシデントを調査するために、「mfa」、「okta」、「2fa」などのキーワードを使用して、MFA を模倣した類似ドメインの遡及分析を実行しました。私たちの調査では、2022 年初頭にかなりの数の類似ドメインがこれらの攻撃に利用されていましたが、幅広いターゲットと 2022 年 7 月から活動が明らかに増加していることがわかりました。1,600 を超えるドメインに、企業機能と MFA に類似した機能の組み合わせが含まれていました。ターゲットは、Coinbase、Reddit、Twilio などの報告されている大企業から、大手銀行、ソフトウェア会社、インターネットサービスプロバイダー、政府機関、世界中のゲームプラットフォームまで多岐にわたりました。また、小規模なテクノロジー企業、食料品店、小売業者も標的とされましたが、あまり報告されていませんでした。

あまり知られていないターゲットの例として、複数の MFA に類似したドメインが Western Electrical Coordinating Council (WECC) を模倣しました。
WECC は、米国西部における広域の電力系統の安定性を促進しています。類似ドメインには wecc-okta[.]org、wecc-oktc[.]org、wecc-okta[.]com などがあります。いずれも 2023 年 2 月に登録され、共通の IP アドレスです。

もう 1 つの驚くべき例は、Feldman Auto Group で、米国内の複数の自動車ディーラーで構成されています。
同社は米国の俳優 Mark Wahlberg 氏とブランド提携をしていますが、それ以外は中西部に 18 の拠点を持つ中規模企業です。[19] このドメインの MFA に類似したドメインである、feldmanauto-okta[.]com は、2023 年 1 月下旬に登録されていました。

MFA の類似ドメインのターゲットとなる企業の中には、より不明確なものもあります。
frb-okta[.]com というドメインは、Federal Reserve Bank、First Reserve Bank、またはポーランドの衣料品会社、Farbokta のようなサイトに類似した平凡な FRBOkta のロゴとログイン指示を表示します。[20] 多くのケースでは、標的の対象がなんであるのか不確かで、フィシングキットが短期間のみ有効になっています。
図 3 にはログインのスクリーンショットが含まれているので、ご自身で推測してください。

これらの AitM 攻撃は、2022 年にも消費者、特に MFA を使用してゲーム内購入を保護するゲームコミュニティの消費者に対して使用されました。
著者らが知っているあるケースでは、被害者は人気オンラインゲームの Twitch ライブ配信からサイトに誘導されるというものでした。MFA 認証情報を入力した後、自宅ネットワークに対して短時間のサービス拒否 (DoS) 攻撃を受け、数分間インターネットが停止しました。ゲームアカウントに戻れた時には、購入したものがすべて盗まれていました。私たちは、ゲーマーは親の地下室に住む 10 代の若者だと考えているかもしれませんが、アプリ内課金に費やされる金額が高額のため、Roblox から Counter-Strike に至るまで、ゲームとそのプレイヤーは有利なターゲットとなっています。

FRBOKTA.COM MFA の類似

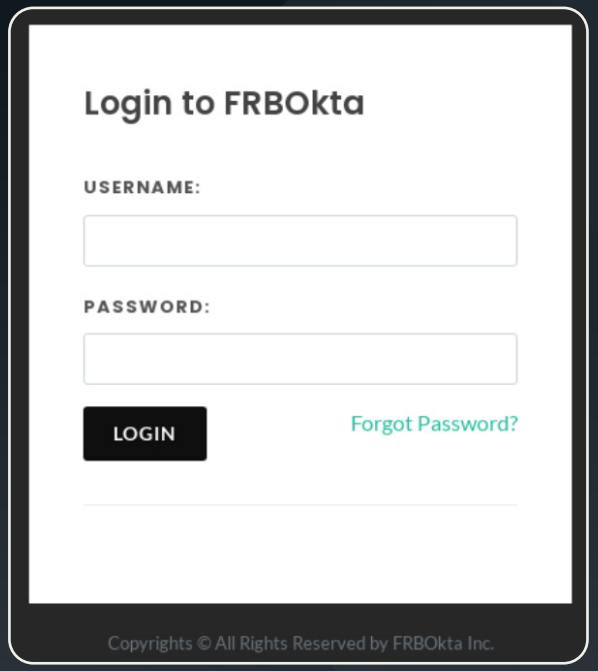


図 3. frb-okta[.]com の Web サイトには、FRBOkta への言及がある何の変哲もないログインページが表示されています。画像著作権 : URLScan[21]

トルコの官庁の類似ドメイン

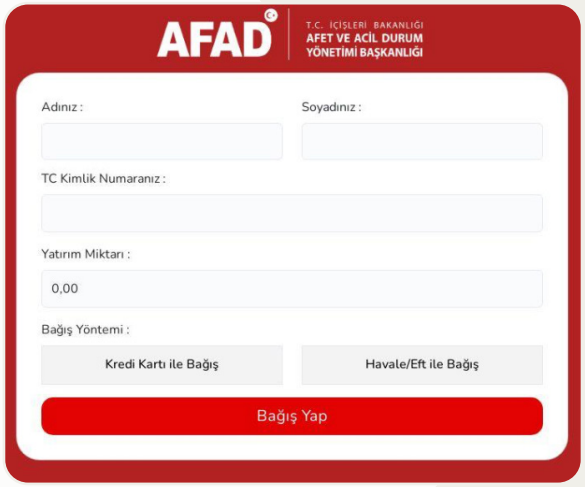


図 4. AFAD 類似ドメイン afadestek[.]net
画像著作権 : DomainTools

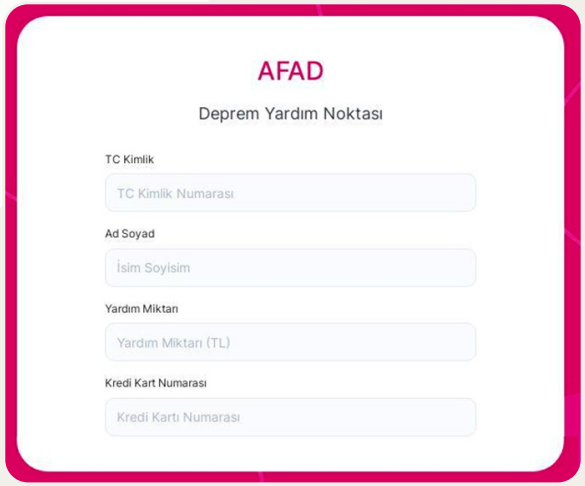


図 5. AFAD 類似ドメイン afadbagislari[.]net
画像著作権 : DomainTools

善良な人が狙われる

お金を盗もうとする詐欺師は、不正手段で利益を得るために、世界の出来事や災害を利用して「最初の対応者」となることがよくあります。

Infoblox では、詐欺師が新型コロナのような健康危機やロシアのウクライナ侵攻など、ニュースのあらゆる出来事をすぐに利用することを発見しました。残念ながら、2023 年は 2 月上旬に発生したトルコ・シリア地震で人道危機に見舞われました。[22] 2 月 6 日の最初の地震の後、いくつかの不正なドメインがトルコ内務省の災害緊急事態管理庁 (AFAD) の Web サイトを模倣しようとしました。これらのドメインは、完全修飾ドメイン名で「AFAD」を利用し、正規のドメイン afad[.]gov[.]tr のように見せようとしていました。以下の例は新たに登録されたドメインであり、長い完全修飾ドメイン名 (FQDN) ですが、すべて「AFAD」で始まります。

より長い FQDN を使用すると、詐欺師は、AFAD をテーマにした複数の組織的活動で使用するために、正規のドメインをさらに並べ替えることができます。

- **afad-kizilay[.]yardim-yap[.]net**
- **afad-kizilay[.]yardimbagis[.]net**
- **afad-online-odeme-bagis[.]net**
- **afadtr[.]bagislama[.]net**

コンボスクワッティングに加えて、これらのサイトの一部は正規の AFAD ロゴを使用して、訪問者を騙してサイトに寄付させるように誘導しています。例えば、詐欺サイト afadestek[.]net は、2 月 7 日に登録され図 4 のように、正規のトルコの AFAD サイトの Web デザインに似せて表示されていました。機械翻訳によると、クレジットカードや電子送金による郵便為替で寄付を集め、姓名や国民 ID 番号などの個人情報も収集しているようです。

他の不正なドメインは、AFAD の公式ロゴをわざわざ使用せず、寄付者から引き出せる金額を最大化するために急いですべてをまとめていました。2 つの例は afadbagislari[.]net と afadyardimyap[.]net でホストされ、どちらも同じ IP アドレスでホストされていました。類似ドメイン専用のインフラストラクチャは一般的で、後でさらに詳しく説明します。どちらのサイトも、図 5 に示されているのと同じレイアウトと内容で、クレジットカード決済で地震救援のための寄付を呼びかけています。

暗号通貨がターゲット

手っ取り早く金儲けを狙う詐欺師とは別に、認証情報を盗むためにも類似ドメインが頻繁に利用されています。

ユーザーから認証情報を得ようとする一般的な「フィッシング」ウェブサイトと言えば、思い浮かべるのが類似ドメインでしょう。暗号通貨の人気上昇に伴い、攻撃者はマーケットプレイス、ウォレット、取引所を含むこれらの金融サービスを標的にしています。私たちは、米国を拠点とする人気の取引所である、Coinbase の非常に説得力のある類似サイトを多数見つけました。そのようなサイトの 1 つを図 6 に示しています。[23]

例えば、下の表のドメインは 2023 年 1 月に登録されていました。

表 1. Coinbase 暗号通貨取引所の類似ドメインの例。	
securefinancialcoinbase[.]com	reconfirminfocoinbase[.]com
secureaccountreverify-coinbase[.]com	reconfirmaccount-coinbase[.]com
secure4-coinbase[.]com	kyc-reverifycoinbase[.]com
secure2reconfirm-accountcoinbase[.]com	ap-coinbase[.]com
secure2financial-coinbase[.]com	accountupdate-financialcoibase[.]com
secure2-financialcoinbase[.]com	2farecoverycoinbase[.]com
secure-2faupdatecoinbase[.]com	recovery-financialcoinbase[.]com
2fa-accountupdatecoinbase[.]com	2fa-updatecoinbase[.]com

2023 年 2 月に取引が 20 億 ドル以上に達した NFT (非代替性トークン) の成長に伴い、攻撃アクターは投資家から資金を盗むために、従来の暗号通貨以外にも素早く拡大しました。[24]
一例として、Blur マーケットプレイスは 2022 年 10 月にオープンし、Blur トークンはその数カ月後に発売開始となり、2022 年 5 月以降、NFT への投資が記録的に増加しました。[25] 商品の発売後すぐに Blur の類似ドメインを私たちは確認し始め、その後、プラットフォームが人気になるにつれ、類似ドメインの劇的な増加も確認しました。

COINBASE の類似ドメイン

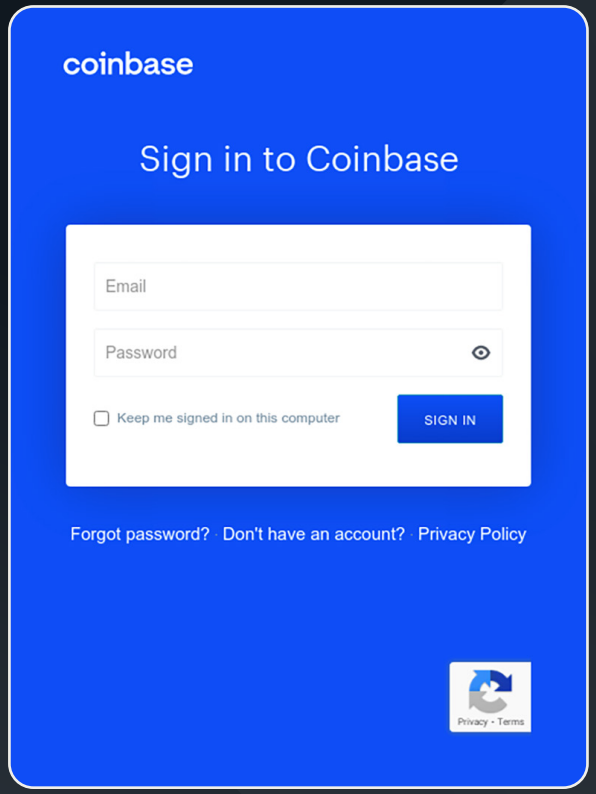


図 6. Coinbase の類似ドメイン click-coinbase[.]com
画像著作権 : DomainTools

BLUR NFT の類似ドメイン

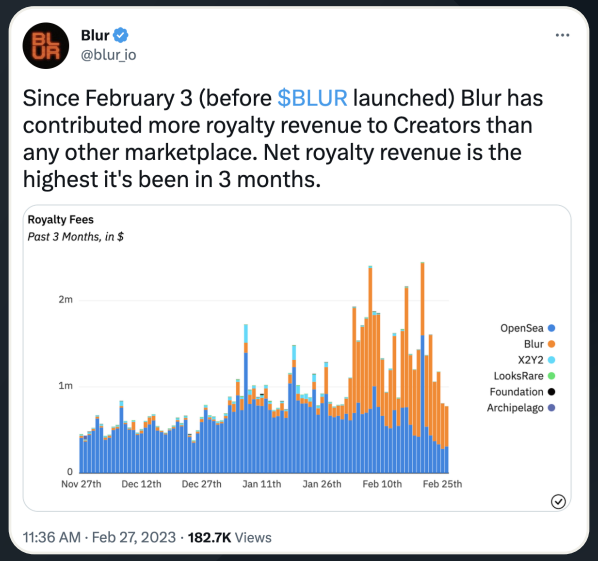


図 7. Blur の NFT マーケットプレイスは、2023 年 2 月に見られた 20 億ドルの NFT 取引を牽引しています。[26]
画像著作権 : Infoblox

2023 年 2 月 14 日の Blur トークン発売開始までの間に、Blur 関連の類似ドメイン数が 5 倍から 6 倍に増えたのを確認しました。 その数は減少していますが 2023 年 3 月の時点では、このパターンは、手っ取り早く金をだまし取るために、暗号通貨の世界のトレンドに遅れを取らないようにする攻撃アクターの意欲を示しています。

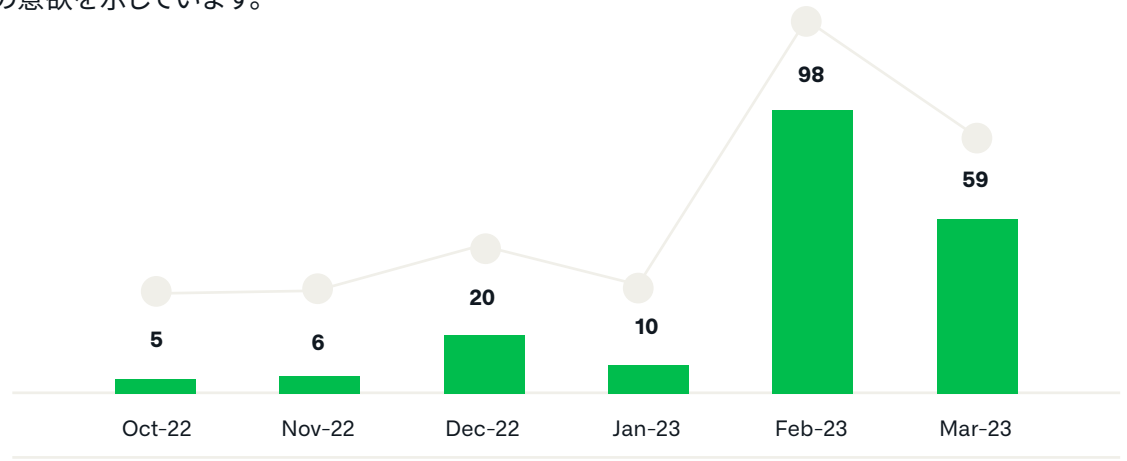


図 8. 2022 年 10 月のマーケットプレイスの発表以降、Blur 関連の類似ドメインが激増。

Infoblox は、仮想通貨関連の類似ドメインを専門とする複数の攻撃アクターを追跡しています。これらのアクターは、Blur とその競合他社、ApeCoin と人気の NFT Bored Ape Collection の所有者である Yuga Labs を含む、市場のすべての主要な組織をターゲットにしています。以下の表では、これらのドメインのごく一部をご紹介します。 これらのアクターが使用する手法には、トップレベルドメイン (TLD) の単純な変更、一文字を追加、Unicode ドメイン名の追加などが含まれますが、これらは特に識別が困難な場合があります。以下の表では apecoíns[.]com の「i」にアクセントがあることに注意してください。DNS では、このドメインは xn--apecons-cza[.]com のように見え、類似しているドメインとして認識するのはやや困難ですが、Web ブラウザでは元のドメインと事実上区別できません。

表 2. Blur トークンと Yuga Labs の類似ドメインの例。

Blur の類似ドメイン [blur.io]	Yuga Labsの類似ドメイン [yuga.com]
blurclaim[.]com	yugaslabs[.]com
blurdrop[.]com	apecoíns[.]com
blurnft[.]pw	apecoinstake[.]world
blur-nft[.]org	yugas[.]app
blur-coin[.]com	ape-claim[.]com

また、ターゲットをドメインに誘導する進路として YouTube を使用する、従来とは異なる暗号通貨関連の類似ドメインもあります。

これらの構想は、脅威アクターが正規の製品に関連しているように見える偽のスポンサーシップの提供を使用して、人気のある YouTube クリエイターをスピアフィッシングすることから始まります。[27]

このメールは、クリエイターが、宣伝しているソフトウェアのコピーやスポンサー契約を含む PDF ファイルなど、スポンサーシップの提供に関連しているとされるファイルをダウンロードして開くように促します。[28] 実際には、これらのファイルはマルウェアのペイロードであり、開くと被害者のブラウザからセッション Cookie を盗みます。盗まれたクッキーから多要素認証が有効になっている場合でも、攻撃者が被害者の YouTube アカウントにアクセスできるようになります。

攻撃者はクリエイターの YouTube アカウントにアクセスすると、Elon Musk 氏や彼の会社の 1 社に関連することが多い、名前とプロフィール写真を変更することで、チャンネルがハッキングされたという事実を隠蔽しようとします。[29]

攻撃者は、さらにその痕跡を隠すために、チャンネルの既存の動画を削除または非表示にすることもあります。その後、攻撃者は、チャンネルの既存の加入者を誘い込むために、Elon Musk 氏の Ark Invest のスピーチなど、暗号通貨関連の動画の編集版の配信を開始します。

これらの編集された動画には、ユーザを攻撃者の暗号通貨関連の類似ドメインにアクセスするように指示するテキストオーバーレイが含まれており、配信の説明にもドメインへのリンクが含まれています。

ドメイン自体は標準的な「お金を倍増させる」詐欺であり、被害者に特定のウォレットアドレスに一定額の暗号通貨を送信するよう促し、その金額の 2 倍を受け取ることを約束するものです。これらの攻撃では、類似ドメインの目的は、編集された動画でそのテーマに合わせて、YouTube チャンネルのブランドを新たにして、提供するものについての信頼性を高めることです。

TESLA の類似ドメイン

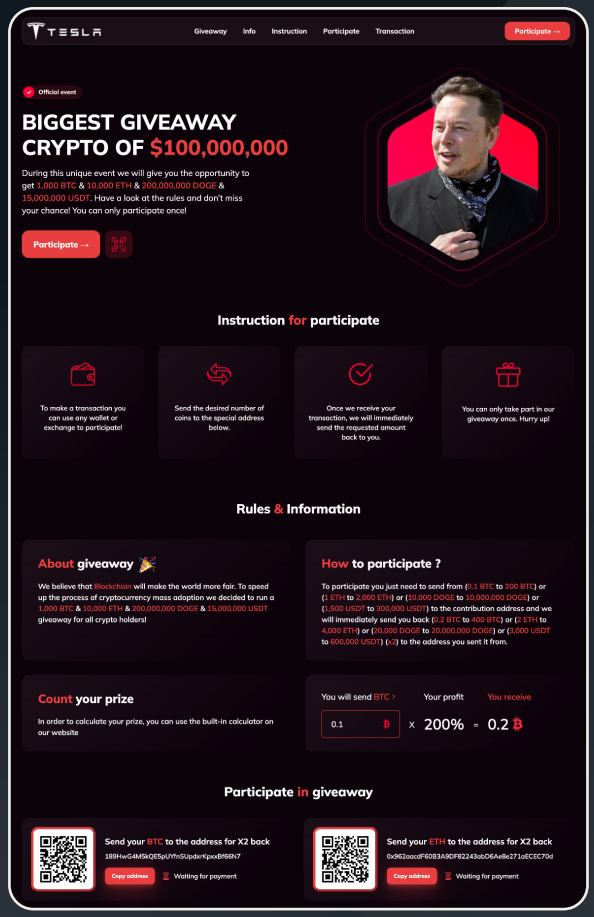


図 9. 2 倍の見返りを受け取るために特定のアドレスに暗号通貨を送信するようユーザに促す、暗号通貨関連の Tesla 類似ドメイン。画像著作権 : Infoblox

ソーシャルメディアとモバイルユーザがターゲット

Instagram や Twitter のようなソーシャルメディアプラットフォームや、Apple のような大手ブランドも、フィッシングのための類似ドメインのターゲットとして人気があります。

すべての人気のあるブランドやサービスが継続的にこれらの攻撃の標的となっていますが、現在の脅威を説明するために、これら 3 つのブランドからほんの数例を使用します。認証情報の収集は新しいものではありません。ソーシャルメディアや Apple ID などのユニバーサル ID プラットフォームが登場する前、悪意のあるアクターがメールアカウントに侵入しようとしていました。しかし、ソーシャルメディアとユニバーサル ID プラットフォームが私たちの生活に深く関わっている現在、これらの類似ドメインは絶えることない脅威となっています。

脅威アクターは、インフルエンサーや有名人のアカウントだけでなく、あらゆる人のソーシャルメディアアカウントを狙います。Instagram には、コンボスクワットもあれば、ホモグラフもあるなど、類似ドメインがたくさんあります。多くの場合、このようなドメインは同時に登録されたドメインのクラスターとして出現し、DDGA を使用して作成された連係している組織的活動の一部であるように示唆されていました。以下の例はすべて、ブランドとヘルプやフィードバックなどの単語を組み合わせた Instagram セットの一部です。

表 3. Instagram サポートの類似ドメインの例。

help-instagram-notice[.]com	help-instagram-about[.]com
feedback-instagram[.]com	help-Instagram-notice[.]com
help-Instagram-about[.]com	help-Instagram-notice[.]gq

これらのドメインのコンテンツは、ユーザが Instagram の著作権規則に違反していると主張し、その裁定に異議を申し立てるためにユーザ名を入力するようにユーザに求めています。図 10 と 11 を参照。

INSTAGRAM LOOKALIKE

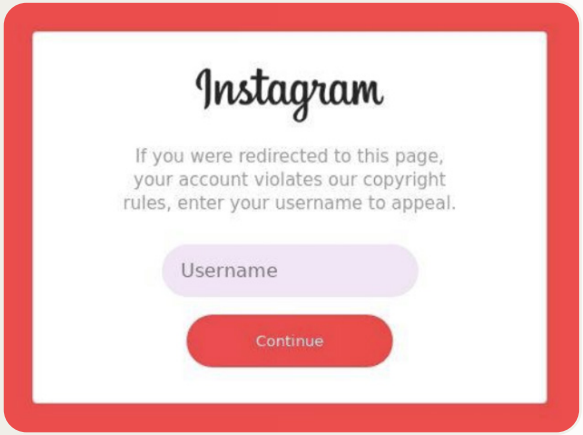


図 10. 著作権侵害の訴えを喚起することを表示している、Instagram の類似ドメイン、help-Instagram- notice[.]com。[30]

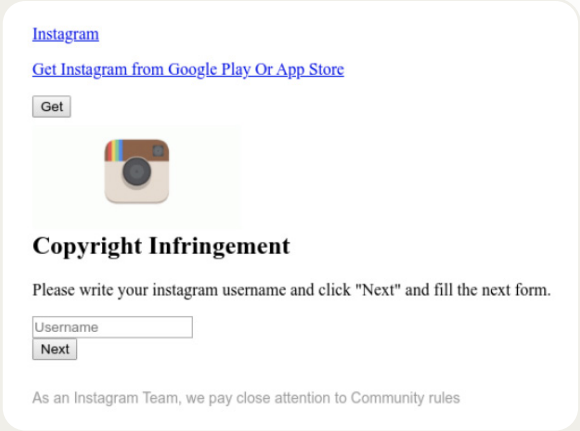


図 11. Instagram の類似ドメイン help-instagram-about[.]com、別の著作権侵害の訴えの喚起を表示。
画像著作権 : URLScan [31]

TWITTER の類似ドメイン

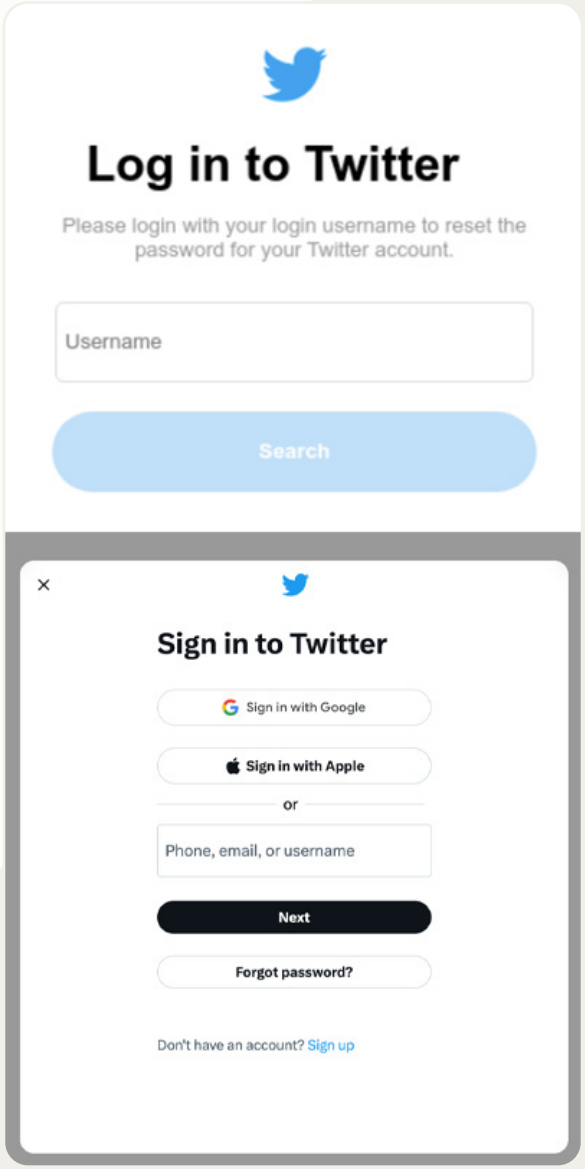


図 12. Twitter の類似ドメイン help-twitter-centre[.]net 上の説得力のあるパスワードリセットポータル。上がフィッシング画像、下が正規の画像。
画像著作権 : DomainTools[32]

他の Instagram の類似ドメインは、大文字の「i」の代わりに小文字の「L」を使うことで、人気の「青いチェックマーク」(Instagram が公式で本物であることを証明する仕組み) を狙っています。
皮肉なことに、Instagram はなりすましに対抗する方法として、有名人や企業に青いチェックマークを導入しました。類似ドメイン対策ソリューションを狙う類似ドメインを利用する悪質なアクターを見過ごすことはできません。

以下はいくつかの例です。

表 4. Instagram の認証の類似ドメインの例。	
Instagram-blueticket-form[.]ml	Instagram-contactbluebadge[.]ga
Instagram-verification-badges-service[.]com	Instagrambluetickverifcation[.]cf
Instagramverifybadge-contact[.]cf	Instagram-badgecentre[.]gq

Instagram の類似ドメインを追跡したところ、攻撃アクターはすべての卵を 1 つのソーシャルメディアのバスケットに入れていないことがわかりました。

Twitter の類似ドメインも、Instagram の「著作権侵害」の類似ドメインと一緒にホストされていました。これらの Twitter の類似ドメイン は、ユーザの認証情報をフィッシングするコンボスクワットドメインで、ランディングページは正規のパスワードリセットポータルのように見えます (図 12 を参照)。

ソーシャルメディアの類似ドメインに加えて、私たちの調査中には、クラウドストレージと Apple デバイス間での同期を提供する Apple のクラウドサービスである iCloud の類似ドメインもよく目にしました。これらのドメインは比較的少数のキーワードを利用していました。最も頻繁に観察されたのは、「apple」、「findmy」、「id」、「icloud」でした。Apple 関連の類似ドメインが不足することはありませんでした。

以下にいくつかの例を示します。これには、スペイン語圏のユーザをターゲットにしていると思われるものも含まれています。

表 5. Apple 関連サービスをターゲットとする類似ドメイン。	
supportid-apple[.]com	sopport-apple[.]com
soporte-latam[.]us	soporte-appleid[.]com
lcloud-web-app[.]com	icloud-fndmy[.]com

すべての人がターゲット

当社の検出アルゴリズムは、毎日何千もの新しい類似ドメインを識別しています。
規模の大小を問わず、悪意のあるアクターが金銭や個人情報を盗むことができるあらゆる企業やサービスが標的となります。このセクションの最後に、実際に観察されたさまざまな類似ドメインとそのターゲットを紹介します。

表 6. 類似ドメインとそのターゲット。

類似ドメイン	類似ドメインのターゲット
mee6bot[.]ru	Discord ボット、Mee6
vulcan[.]pm	Discord ボット、Vulcan
o365-outlook[.]com, ms-o365[.]com, o365-outlook[.]com, https-o365[.]com	Microsoft Office 365
myato-refund[.]online	オーストラリア税務署
checkscam22[.]com, checkscams[.]online, checkscammer[.]xyz	詐欺チェックサイト
xpressvpn[.]business, expressvpn-app[.]com, expressvpn-okta[.]com	Express VPN
anpost-paymentduty[.]com, ups-pay-deliveryfee[.]info, caddeliverypostca[.]com	郵便・宅配サービス
crarebate-info[.]com	カナダの税金還付
ebl-ch[.]com	スイスのエネルギー会社 EBL
op-fi-palvelut[.]co, op-fi-io[.]in	Op[.]fi、フィンランドのデジタルバンキングおよび保険サービス
boatairbuds[.]in, boatbudsmusc[.]in, boatflashsale[.]in, boatmusicairbud[.]in	インドのテクノロジー企業、BoAt
pumauaeshoes[.]com, pumanzsale[.]com, pumaireland[.]com, vejaoutletcanada[.]ca	靴会社
secure1-scotiabank[.]com,r-scotiabank[.]com, chasebank-jpm[.]com, thetrustnationalbank[.]com, amėricafirst[.]com	銀行
sprint-ldg[.]com, tds-telecom[.]com, teistra[.]ne, 1111systems-okta[.]com, t-mobile-okta[.]us, vzw-sso[.]com	Internet およびクラウドサービスプロバイダー
sso-authentication[.]de, sso-securelogin[.]com, service-sys-2fa[.]com	多要素認証とシングルサインオンのドメイン

類似ドメインはどのように使われているのか

類似ドメインとは何か、そしてターゲットの例をいくつか取り上げました。次に、類似ドメインがどのように使用されるかについて説明します。

「どのように」とは、その展開方法を意味します。Infoblox では、類似ドメインが次のような様々な方法で展開されていることを確認しました。

- **SMS メッセージ**
- **電話をかける**
- **ソーシャルメディアサイトでのダイレクトメッセージ**
- **メール**
- **QR コードへの埋め込み**
- **World Wide Web 上のドメイン**

SMS を送ってきます

携帯電話のテキストメッセージ (SMS) のスパムフィルターが改善されたにもかかわらず、フィッシングメッセージ (スミッシングと呼ばれることが多い) を配信するための SMS の使用は増え続けています。

脅威アクターは、大量のメッセージをすばやく配布し、メールフィッシング攻撃から保護するために導入されているセキュリティメカニズムの一部を回避することができます。SMS は、広範な消費者攻撃と、組織の従業員に対する狭い範囲のスピアフィッシング攻撃の両方で使用されます。このセクションでは、SMS と類似ドメインを使用して消費者と政府職員を攻撃した 2 人の攻撃アクターについて説明していきます。

Infoblox は、ほぼ 1 年にわたり、執拗に類似ドメインのスミッシングを行う攻撃アクターを追跡してきました。私たちは、その攻撃アクターを OpenTangle と名づけました。 私たちの知る限り、このアクターは他の場所では報告されていません。OpenTangle は当初、金融機関、インターネットプロバイダー、オンライン小売業者の類似ドメインを使用して、欧米の消費者をターゲットにしていました。この攻撃アクターは最近、政府関連組織の職員や請負業者を標的にし始めました。約 2 年前に OpenTangle が運用を開始して以来、1500 以上の類似ドメインが OpenTangle によって管理されていることを確認しています。OpenTangle のいくつかのドメインには、mtbsuportz0610[.]com、americafirst0nline[.]com、mygov03-ato[.]com があります。.

様々な類似技術を使用していることに注目してください。

このレポートの著者の一人は、著者が関係していない M&T Bank の類似ドメインを含む複数の SMS を OpenTangle から受け取っています。OpenTangle の組織的活動の初期段階には、難読化が成功することを期待して、短縮された URL リンクをスミッシングテキストに含めていました。しかし、2022 年 5 月までには、類似ドメインに変換されました。図 13 は、ユーザの認証情報を要求する銀行に関する組織的活動の 1 つの例を示しています。

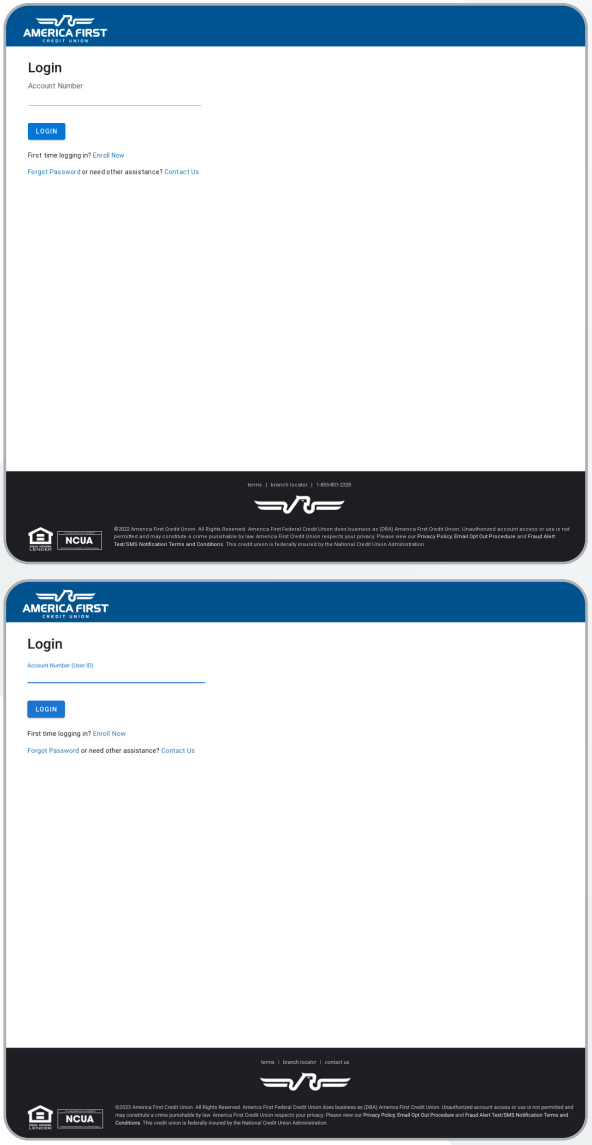


図 13. America First Credit Union の口座保有者を狙ったドメイン americafirst0nline[.]com のフィッシングページ。上の画像はフィッシングページ、下の画像は正規のページ。
画像著作権 : URLScan[33]

OpenTangle は、昨年中に AitM フィッシングキットを使用して MFA の悪用を開始しました。
初期の組織的活動では標準的なフィッシングログインページを使用し、一般消費者をターゲットにしていましたが、図 14 はその組織的活動が進化されていることを示す例です。このケースでは、オーストラリア政府の myGov アカウント保有者をターゲットにして、単純なログインではなく、MFA コードを要求しています。また、ヘルプデスクに電話するためのリンクが含まれていますが、これもユーザに悪意のあるウェブサイトを閲覧させる手段として 2022 年に登場した手法です。

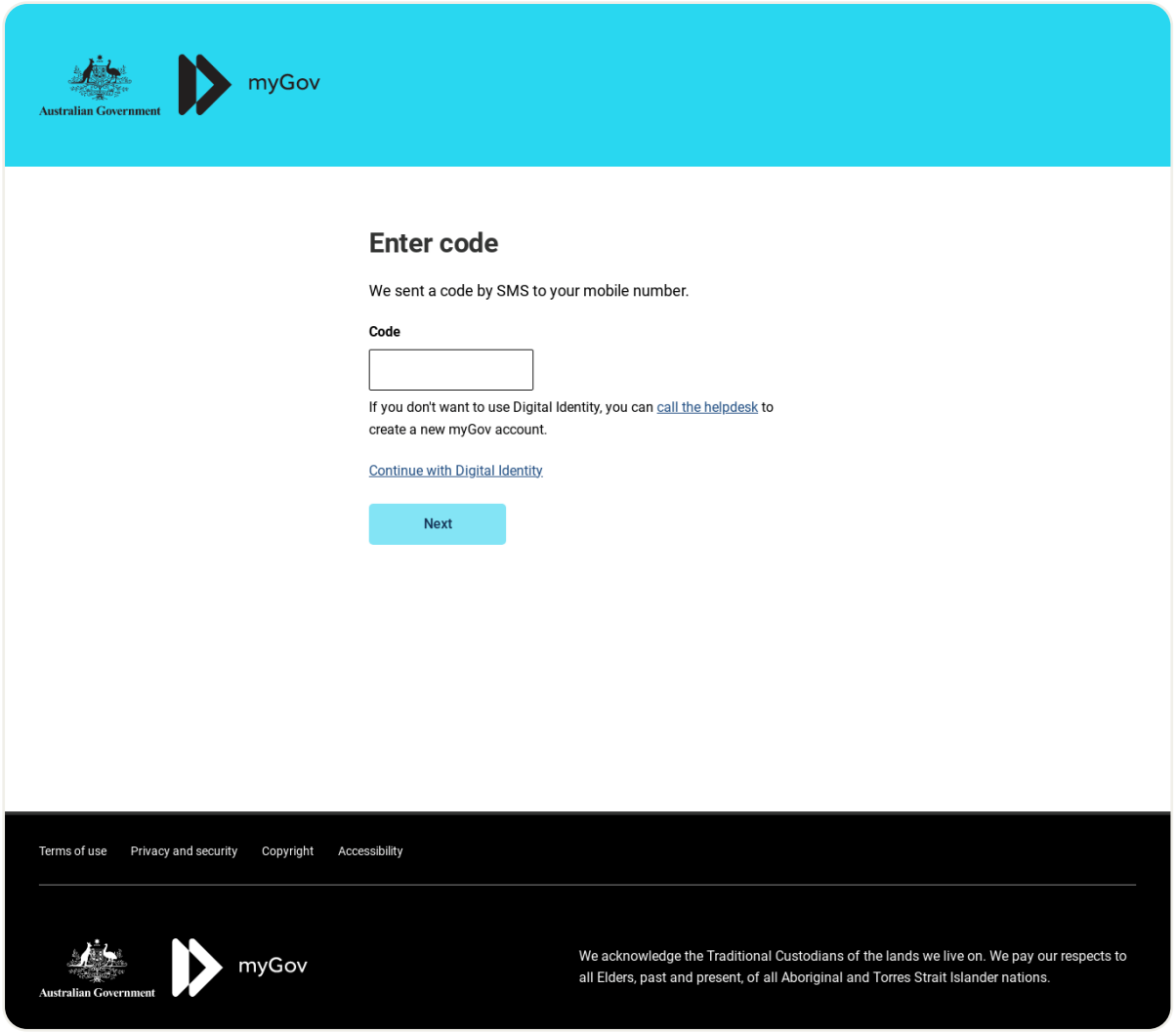


図 14. オーストラリア政府のクラウド用オンラインポータルである myGov を模倣した OpenTangle による類似ドメイン www.mygovsupport-ato[.]com。画像著作権 : URLScan[34]

Scamélie も、スミッシングメッセージを使用して類似ドメインを拡散する攻撃アクターの例です。

私たちが Scamélie と呼ぶこの攻撃アクターは、主にフランス語圏の国をターゲットとした詐欺の多くに関与している、緩やかに連携しているグループや個人の集まりです。また、彼らがヨーロッパとアラブ首長国連邦全体で、もっと様々に標的を絞っていることも確認しています。Scamélie の類似ドメインは、主に ISP、銀行、政府サービス、配送会社を模倣しています。グループの連携が緩いため、旅行会社、スポーツアパレル会社、食料品店など、あまり予想していないような企業に対する詐欺も目撃されています。

Scamélie の類似ドメインは、多くの場合、大規模なクラウドプロバイダーや「防弾」ホスティング会社でホストされています。また、詐欺師が独自に設定した場合や、無関係の他の詐欺師が設定したホスティングプロバイダーを使用している場合もあります。私たちは、標的とされたドメインだけでなく、盗まれた ID によって登録され、仮想クレジットカードや暗号通貨で支払われた汎用ドメイン（my-account、resolve-an-issue など）の両方で確認しました。

攻撃アクターはクレジットカード情報を収集すると、被害者の銀行またはクレジットカード発行会社の従業員を装って被害者に電話をかけます。
彼らは、被害者のクレジットカード情報が盗まれているが、問題の解決に協力すると説明します。次に、被害者は 2 つの MFA コードを受け取り、アカウントのセキュリティのために発信者にこれらのコードを読み戻す必要があると伝えます。実際には、攻撃者は被害者からリアルタイムで金銭を盗むために MFA コードを必要とします。最初の MFA コードにより電信送金額を増額させ、2 番目の MFA コードにより電信取引の実行が可能になります。電話での効果を高めるために、攻撃アクターは次のような電話をかけます。理想的には、ネイティブスピーカーかどうか疑われない方法でフランス語を話す若い女性および / または個人が電話をかけてきます。

Scamélie は組織化されていないグループであるため、追跡と分析が困難です。多くの場合、被害者の夜間の時間にスミッシングを行い、わずか数時間または数日後にドメインを削除します。彼らは、アンチボットとアンチスクレイピングスクリプトを使用して、セキュリティ調査をさらに妨害します。

SCAMÉLIE 類似ドメインの例

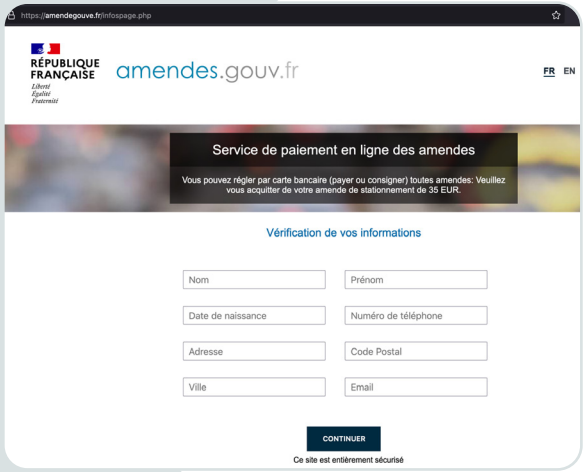


図 15. フランス政府のサービスポータルを模倣した Scamélie の類似ドメイン amendegouve[.]fr。
画像著作権 : Infoblox。

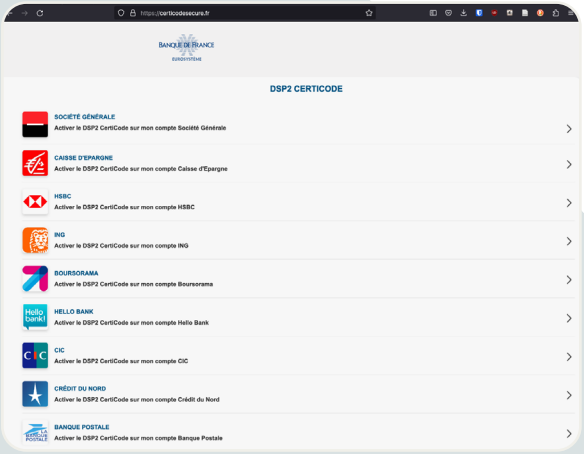


図 16. Scamélie の類似サイト certicodesecure[.]fr は、フランスの銀行サービスを模倣して、被害者に銀行口座情報をリンクさせようとします。
画像著作権 : Infoblox。

昔ながらの手法である電話が使用されます

CISA (サイバーセキュリティインフラセキュリティ庁) は、2023 年 1 月 26 日に、リモート監視と管理ソフトウェア (RMM) の悪意ある使用に関する CSA (サイバーセキュリティ勧告) を発表しました。[35]

CISA は、2022 年 10 月に、悪意のあるアクターが電話番号を含むフィッシングメールを送信し、ユーザに電話するよう促す組織的活動を特定しました。このメールはカスタマーサポートからのメッセージとして送信されるように設計されており、ユーザがその電話番号に電話をかけると、攻撃者は悪意のあるドメインにアクセスするよう促しました。ユーザがその通りに実行すると、実行可能ファイルがダウンロードされ、次に 2 番目の悪意のあるドメインに接続され、そこから追加の RMM ソフトウェアがダウンロードされました。このソフトウェア (AnyDesk と ScreenConnect) は正規のものですが、一貫して攻撃者の RMM サーバーに接続するように事前設定されていました。

使用されているドメインは、よく知られたサービスの類似ドメインで、スクリプトや発信者のペルソナの作成にソーシャルエンジニアリングが追加で使用されているため、電話でドメインを知らされた被害者の場合、ドメインを受け入れる可能性はさらに高くなります。データを遡及的に見直したところ、CSA が示すよりも長く活動しているという証拠が見つかりました。[36] これらの組織的活動は、インシデントの 1 年以上前の少なくとも 2021 年春から活発に行われていたと、CISA と Silent Push が別の記事で説明していました。また、ドメインの再利用も確認されたということでした。例えば、ドメイン amzsupport[.]live という Amazon の類似ドメインは、2020 年 4 月に活発な組織的活動の一部として使用され、2021 年 10 月に再び使用されました。

企業内部システムの MFA 保護に対する攻撃が 2023 年の早い段階で明るみに出たため、一部のケースでは、攻撃アクターが IT 部門を装い、被害者に電話をかけていたことが明らかになりました。これは、被害者が最初の指示に応答しなかった後に行われ、ユーザが類似ドメインにアクセスする必要性をさらに正当化するために使用されました。これに従ったユーザにより、攻撃アクターは企業の認証情報を盗むことができました。

スパムメールを送信してくる

狡猾な攻撃アクターがスミッシングや電話を利用して類似ドメインを配布し、被害者を罠にかけるのを目撃してきましたが、フィッシングメールが時代遅れになることはありませんでした。

Infoblox は毎日数万件の悪意のあるスパムメールを分析し、類似したドメインを配布する組織的活動が絶え間なく続いていることを明らかにしています。これらの組織的活動のいくつかに焦点を当てますが、組織がフィッシングメールに対する丹念な監視を続けることの重要性を強調していきます。

そのような組織的活動の 1 つでは、米国の大手通信会社である Xfinity が標的にされています。これらの類似ドメインは DGA に似た特徴があり、xfnity< 略語または一部の単語 >.com という形式です。最初の「i」が欠落していて、「Xfinity」のスペルが間違っていることに注意してください。この攻撃アクターはまた、送信者名が正当なものであるように見せるために、キリル文字の大文字「X」を使用した「Xfinity Mobile」と表示していました。送信者のメールは独自のドメインを使用しており、ユーザ名にも DGA のような特徴があり、noreply-(noreply-corporate@xfnitycard[.]com など) というパターンで構成されているようです。攻撃アクターは、各メールに固有のドメインを使用していませんでした。一部の例では、noreply-corporate@xfnitycard[.]com や noreply-active@xfnitycard[.]com のように、ドメインは繰り返し使用されていましたが、キーワードを変えていました。

表 7. Xfinity の類似ドメイン。

xfnitykuri[.]com	xfnitycomp[.]com
xfnitystarter[.]com	xfnityhlaty[.]com
xfnityersa[.]com	xfnityothie[.]com
xfnitykaris[.]com	xfnityrkles[.]com
xfnityrayton[.]com	xfnitycard[.]com

この組織的活動で確認されたドメインは、私たちが「おとり駐車」と呼んでいる手法を利用しています。これは、ドメインが直接訪問され、停止しているように見えても、実際にはドメインのメールサーバーが稼働していて、悪意のあるメールを送信しているというものです。私たちは、おとり駐車がかなり一般的であり、他のベンダーによって報告されていないことを発見しました。おとり駐車ページの例については、図 17 を参照してください。

XFINITY の類似ドメ

図 17. Xfinity の類似ドメイン、xfnityrayton[.]com のおとり用保留ページ。画像著作権 : URLScan[37]

WEDO MACHINERY の類似ドメイン

Dear you

Good day !
How are you?
How is your project going?
Do you receive my message?

Hope we can establish long term cooperation.

We got recommendation of your company from our UK partner about

below order as attached

Please confirm if your can deliver the products specifield

Mrs. ConnieXu
Mob: 0086 131 0941 7901 [WhatsApp/Wechat]

Wedo Machinery (Zhangjiagang) CO., LTD.

Add: Zhenbei Road, Leyu Town, Zhangjiagang City, Jiangsu Province, China.

図 18. おとりとして Wedo Machinery とマルウェア C2 として、acrobat-adobe[.]com を使用した、悪意のあるスパムの組織的活動の本文。
画像著作権 : Infoblox

私たちの分析では、配布された悪意のある Word ドキュメントでこれらの Xfinity の類似ドメインが見つかりました。

組織的活動のメールの件名は行動喚起を兼ねており、「【告知】あなたのサービスは終了することになります」や "【要対処】あなたのカードに請求できませんので、このエラーを解決してください」といった、支払い拒否やサービス終了の脅威を中心としたものでした。これらのメールの本文は、カスタマーサポートから送信されたものであるかのように構成され、受信者に「ケースの詳細については添付ファイルを参照してください」と求めていました。

Infoblox が特定した別の組織的活動では、中国のリサイクル企業である Wedo Machinery を使用して、ランサムウェアのローダーを投下していました。 このキャンペーンでは、Zmutzy として識別される単一の実行ファイルを含む .zip ファイルが添付された 176 通のメールが確認されました。組織的活動でのメールの例は、図 18 を参照してください。この組織的活動では、次の 2 つのファイル名が確認されました : PO-0097(1).zip と PO-29862K.zip。Zmutzy ローダーは、類似ドメイン acrobat-adobe[.]com を使用して追加のペイロードをダウンロードします。

QR コードを使っています

直接的な暗号通貨の類似ドメインに加え、次のようなものも観察されました。QR フィッシング（QR コードを使用して URL の宛先を難読化し、悪意のあるコンテンツを配信）と、ユーザに賞品を獲得したと気を引き、暗号通貨ウォレットのアカウント情報を提供するように誘導するために作成された類似ドメインとの併用。

ある例では、QR コードが被害者を bridge[.]walletconnect[.]com のリンクにリダイレクトさせ、資金を盗む仕組みになっていました。この詐欺では、詐欺師が Twitter アカウント、@adidas_weare を開設し、信頼性を高め、類似ドメインを共有しています（図 19 を参照）。このアカウントは、2023 年 2 月 21 日の時点で 16,000 人のフォロワーを獲得していました。幸いなことに、そのアカウントは現在削除または停止されています。

攻撃アクターは、ポルシェの車や Adidas の衣料品や靴を含む様々な商品の偽の景品を宣伝していました。ドメインは、主に「adidas」または「porsche」というキーワードを含むコンボスクワットです。図 20 に示すような類似ドメインにアクセスすると、ユーザは、景品を請求できる QR コードをスキャンするよう求められ、その後、攻撃アクターがユーザの資金にアクセスできるようにする分散型アプリケーション、WalletConnect にリダイレクトされます。

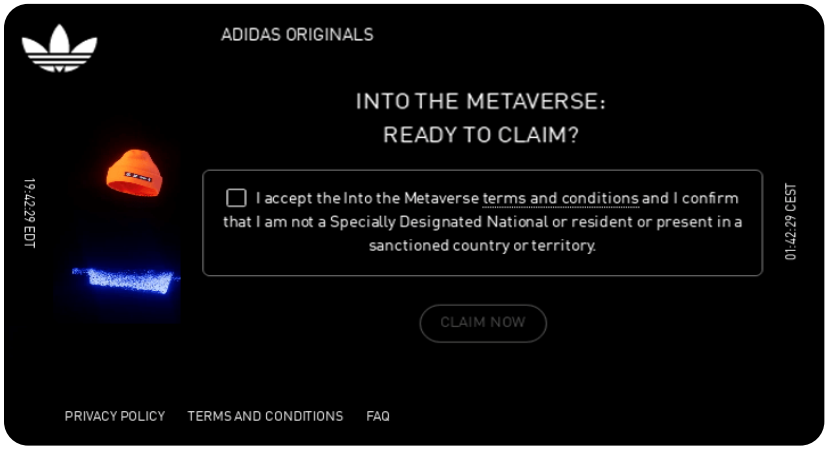


図 20. Adidas の類似ドメイン adidas-go[.]com は、無料の景品を請求するためにクリックするようユーザーを誘導しています。画像著作権 : URLScan[39]

ユーザが QR コードをスキャンし、暗号通貨ウォレットを分散型アプリケーションにリンクすると、攻撃アクターはユーザから暗号通貨を奪うことができます。これらのドメインは共有ネームサーバーを使用し、ロシア語名前解決 IP アドレス 185[.]149[.]120[.]83 でホストされています。この IP アドレスは完全に攻撃アクターによって制御されており、Blur や Ethereum スマートコントラクトの速度とスケーラビリティを向上させるソリューションである Arbitum に類似した他の類似ドメインが含まれています。

ADIDAS の類似ドメ

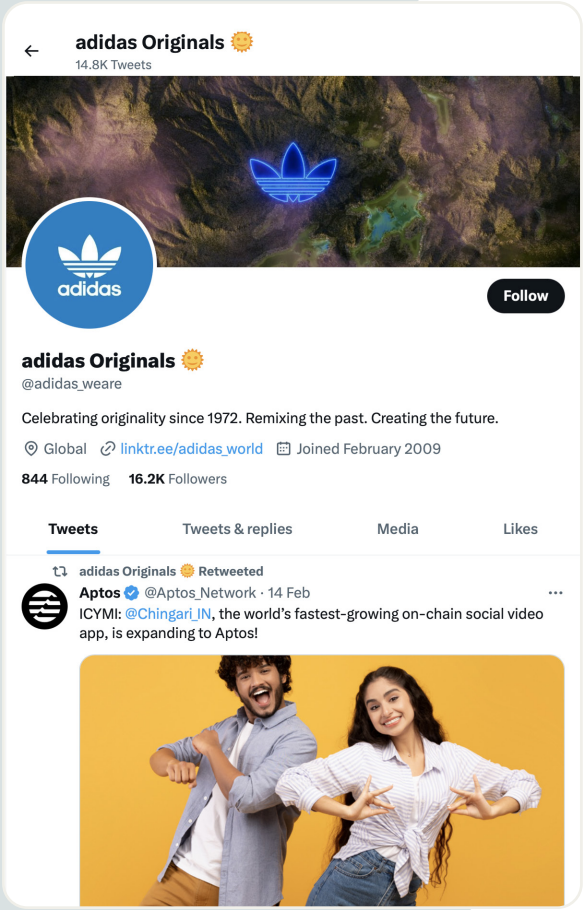


図 19. Adidas Originals @adidasoriginals の類似ドメイン Twitter アカウント @adidas_weare。
画像著作権 : Infoblox

DNS が使われています

Lookalike domainは Web サイトのドメインとしてのみ発生するわけではありません。

次のようないくつかの DNS 機能で使用されていることを確認しました。

- **ネームサーバー**
- **メールサーバー**
- **CNAME レコード**
- **PTR レコード**

ほとんどの場合、これらのドメインには典型的な A レコードや Web サイトは存在せず、停止状態にあることがよくあります。これは、前のセクションで説明したおとり駐車の実装です。攻撃者は、DNS でのリダイレクトや C2 通信にも類似ドメインを使用します。

ネームサーバー

類似ドメインネームサーバーの例として、bitkeep[.]dev と flutter[.]direct のドメインは 2022 年 11 月に登録されました。これらはどちらも異なるドメインに類似していますが、インフラストラクチャを共有しています。BitKeep は、すべての暗号通貨取引の単一のハブとなることを目的とした分散型マルチチェーン暗号ウォレットです。BitKeep の公式ドメインは bitkeep[.]com で、同社は 5 年間運営されており、800 万人以上のユーザがいます。[40] Flutter は、単一のコードベースからモバイル、Web、デスクトップ用のネイティブコンパイルアプリケーションを作成するための Google のポータブルユーザーインターフェース (UI) ツールキットです。Flutter の公式ドメインは flutter[.]dev. です。[41]

どちらの正規ドメインもプライマリドメインで Web コンテンツをホストしていますが、類似ドメインはいずれもホストしていません。最初に登録されたとき、両方のドメインはもう 1 つのドメイン (Flutter の別の類似ドメイン) である、get-flutter[.]com のネームサーバーとして機能していました。当時、ドメインはスイスのオフショアホスティングプロバイダーの Private Layer でホストされていました。このネットワークは、flutter[.]vision もホストしていました。これらのドメインが悪意のある活動によるものであると断定することはできませんが、従来とは異なる目的のために類似ドメインを利用するパターンを示しています。これらは、経験豊富な研究者にとっても分析が非常に困難であることが判明しており、多くの脅威インテリジェンスアルゴリズムをトリガーする可能性は低いです。

メールサーバー

ネームサーバーに加えて、類似ドメインがメールサーバーとしても使用されているのを確認しました。whirlpoolmxonline[.]com と whirlpoolservicesmx[.]com のドメインは、大手家電メーカーの Whirlpool をターゲットにしており、共通のインフラストラクチャを共有しています。これらは、セーシェルにある低品質の VPS とホスティングプロバイダーである Lyra Hosting が所有する同じ IP アドレスでホストされ、同じネームサーバーを共有しています。

第 2 レベルドメイン (SLD) 名で Whirlpool を直接ターゲットにしていますが、他の主要な家電メーカーも同様にターゲットにしていることを示す各ドメイン内の特徴も特定しました。SLD whirlpoolmxonline[.]com には次の 3 個のサブドメインがあります。mabe-onlinemx[.]whirlpoolmxonline[.]com、samsung-onlinemx[.]whirlpoolmxonline[.] com、lg-onlinemx[.]whirlpoolmxonline[.]com。Mabe は、メキシコの家電メーカーです。SLD whirlpoolservicesmx[.]com にはサブドメインがありませんが、ドメインに関連付けられた SSL 証明書の過去のチェーンは、whirlpoolmxonline[.]com と同様の家電メーカーをターゲットにしていることを示しています。www[.]lgservicesmx[.]mabeservice[.]com と *.lgservicesmx[.]com。

メールサーバーとして類似ドメインが使用されると、メールヘッダーを一見しただけで正当であるように見えるため、エンドポイントでフィッシングメールを検出する際にさらに課題が生じます。

マルウェア C2s

先ほどのメール展開のセクションで、Zmutzy ランサムウェアローダーを投下していたことが特定された悪意のあるスパムの組織的活動が、類似ドメイン acrobat-adobe[.] com をマルウェア C2 サーバーとして使用した方法について説明しました。類似ドメインは、正規のドメインと一緒にネットワークトラフィックに簡単に紛れ込むことができるため、マルウェアの C2 に最適です。スロバキアのセキュリティソフトウェア企業である ESET の研究者は2023 年 2 月にメッセージングアプリケーション「Telegram」を装ったマルウェア C2 を特定しました。[42] 歳

Table 8. Telegram lookalikes functioning as malware C2s.

12-03.telegramxe[.]com	12-25.telegraem[.]org
12-25.telegraxm[.]org	12-25.telegraem[.]org

悪意のある .exe ファイルをホストしているドメインは、WhatsApp、Skype、Google Chrome、Firefox だけでなく、Telegram にも類似ドメインでした。

リダイレクト

類似ドメインはリダイレクトとして使用されることもあります。 私たちは、訪問者を choto[.]xyz にリダイレクトするタイポスクワットドメインの大規模なネットワークを特定しました。choto[.]xyz は、被害者を条件付きでランディングドメインの lotto60[.]com にリダイレクトする C2 ドメインです。この攻撃アクターは choto[.]xyz でリバースプロキシサービスと Cloudflare ボットプロテクションを使用し、これはおそらくセキュリティ研究者による検出と調査を防ぐためと思われます。このランディングドメインは、詐欺的なアフィリエイトマーケティングプログラムを実行しているように見えます。ドキュメントオブジェクトモデル（DOM）を分析すると、HTML に、分析 ID G-DT4YWT5VP8 を使用して訪問者データを Google アナリティクスに送信するインライン gtag() 関数が含まれていることがわかります。攻撃アクターのアフィリエイトマーケティングの数字を膨らませるだけでなく、リモートアクセストロイの木馬 Nighthawk であることが確認されたファイル署名と一致する潜在的に悪意のあるファイルによって、lotto60[.]com が HTTP 経由でリクエストされるのを確認しています。[43]

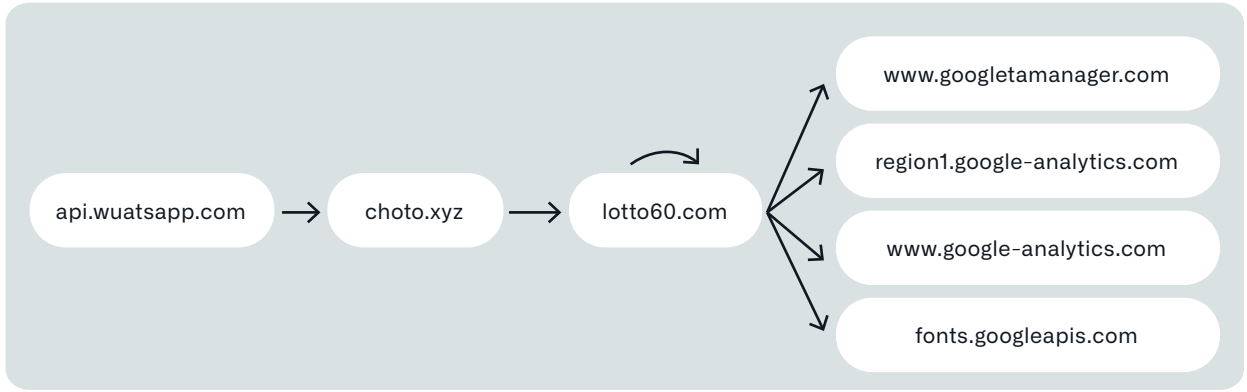


図 21. タイポスクワットドメインから Google アナリティクスへのリダイレクトチェーンの例。画像著作権 : URLQuery[44]

第 1 段階のタイポスクワットドメインは、様々な企業を模倣しています。いくつかの例

表 9. 詐欺的なアフィリエイトマーケティングの組織的活動のリダイレクトとして機能する類似ドメイン。

gi6hub[.]com	whatysapp[.]com
bankofamegica[.]com	babgkokbank[.]com
intuhit[.]com	scotiasbank[.]com

これらのタイポスクワットは通常、リダイレクトとして使用される前に 1 ～ 3 か月間駐車されています。攻撃アクターはこのようなタイポスクワットドメインを作成する際に細心の注意を払っています米国英語の QWERTY キーボードで、間違っているアルファベットはその正しいアルファベットのすぐ隣に位置しています。これらは、平均的に入力している際に 1 日に何度も犯す可能性のある間違いです。ただし、依然として「キーを探しながら入力している」ユーザは別です。

類似ドメインが効果的な理由

読者の皆さん、これまでこのレポートに散りばめられた 19 個の類似ドメインの単語に気づきましたか？（訳註：日本語訳では 1 個のみ）それらのいくつかは見つけるのは非常に難しいです。

ヒント：あと 6 個あります。（訳註：日本語訳ではありません）類似ドメインを見つけることができるかどうかお試しください。

これまで、いくつかの特定のターゲットと、類似ドメインの展開方法のインフラストラクチャについて説明してきました。しかし、なぜそれほど効果的なのでしょうか。なぜこれほどまでに執拗な脅威になるのでしょうか。

その答えは込み入っていて、心理学的な側面や技術的な実装、そして単純な人間のミス（**ミスをするから人間なのですが**）**が関係しています。**

心理言語学

心理学的には、人間の脳は何かを読んでいる時に短絡します (この場合、電流が意図しない最も抵抗の少ない経路を通るという文字通りの定義を意味します)。あなたはおそらく次のようなミームを見たことがあるでしょう。

ケンブリッジ大学の研究者によると、単語の文字の順序は重要ではなく、単語の最初と最後の文字が正しい位置にあることが重要なのです。残りはすべて間違っていても、問題なく読むことができます。これは、人間の脳はすべての文字を一字一句読んでいるのではなく、単語を一つの塊とみているからです (訳註 : オリジナルの英文の単語のスペルはほとんど間違っています)。

ケンブリッジ大学でそのような研究が発表されていないという意味で、この主張は根拠がありませんが、根底にある概念にはメリットがあるようです。例えば、最近の実際の研究では「規則性のないごちゃごちゃした単語を見ると、既知の単語と比較する視覚的表現が活性化する」ことが示唆されています。[45] 心理言語学の根本的な疑問を証明したり反証したりすることは、このレポートの範囲を超えていますが、心理言語学が「類似ドメイン」の効果についていかに重要な役割を果たしているかを示したいと思っています。

特に、ホモグラフィやタイポスクワットに関しては、人間の脳の短絡性が一役買っています。Infoblox[.]com のようなドメインを見たとき、脳は必ずしもそのドメイン名の個々のアルファベットを解析するわけではないので、最初のアルファベットが実際には小文字の「L」であり、大文字の「i」ではないことに気づかないかもしれません。

同じような理由で、ドメインの goooogle[.]com を見ると、あなたの脳は「o」という文字が 2 つではなく 3 つあることを認識しなくなるかもしれません。少なくとも、手遅れになってすでにクリックしてしまうまではそうではありません。

PUNYCODE 対応 : 成り行き任せ

Web ブラウザーには、国際化ドメイン名 (IDN) のホモグラフ攻撃からユーザを保護する方法があります。 最初の、そして最も顕著な防衛線は、Unicode ドメインを Punycode に「翻訳」することですが、Punycode は先頭の「xn--」で認識でき、肉眼では意味不明に見えます。これは、Punycode が Unicode 文字を、文字、数字、ハイフンのみを含む ASCII (American Standard Code for Information Interchange) 文字のはるかに限定されたサブセットにマッピングするためです。主要な各ブラウザは、Punycode ドメインに対応しています。Google は、Chromium でドメインの国際化バージョンと Punycode バージョンのどちらを表示するかを決定するアルゴリズムに関連するヒューリスティックの詳細な説明を提供しています。[46] Mozilla も同様の説明を提供しています。[47]

Mozilla は、IDN 表示アルゴリズムの説明の中で、次のような感動的な記述も提供しています。

> **この問題に対する私たちの回答は、顧客がお互いに盗用できないようにするのは最終的にはレジストリの責任である、というものです。ブラウザは技術的な制限を設けることはできますが、*Web* 上で非ラテン文字のための公平な競争の場を維持しつつ、私たちがレジストリに代わってこの役割を担う立場にはありません。ここで適切なチェックを実行できる立場にあるのはレジストリだけです。私たちの側としては、非ラテン文字を二流市民として扱わないように注意していきたいと思っています。**

2017 年、セキュリティ研究者の Xudong Zheng 氏は、すでに Punycode でドメインを登録しました。xn--80ak6aa92e[.]com は「apple[.]com」と訳され、「apple」のラテン文字の外観を模倣したキリル文字を含んでいます。[48] 当時、Internet Explorer、Microsoft Edge、Safari、Brave、Vivaldi の Web ブラウザには脆弱性はありませんでしたが、Chrome、Firefox、Opera には脆弱性がありました。現時点では、Firefox のみが Punycode の翻訳を継続し、ユーザが攻撃に対して脆弱なままになります (最近、Internet Explorer または Microsoft Edge でドメインをテストしていません)。

PUNYCODE? とは？

Punycode は、Unicode 文字を、より小さく制限された文字セットである ASCII に変換するために使用される特別なエンコードです。Punycode は、国際化ドメイン名 (IDN) をエンコードするために使用されます。

IDN ホモグラフィーを使用した IMESSAGE のスミッシング

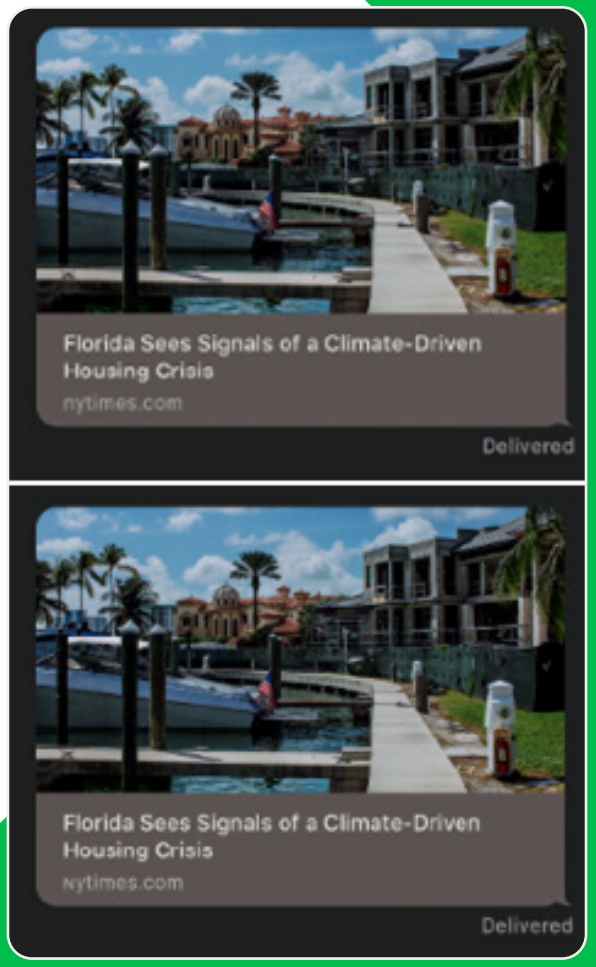


図 22. 上の画像は Tyler Butler 氏が提供したもので、iMessage 経由で送信された実際の New York Times の記事。下の画像は Tyler Butler 氏からの提供で、IDN ホモグラフドメインに関するなりすましの New York Times の記事。
画像著作権 : Tyler Butler

Hu らは、IDN ホモグラフ攻撃に対するブラウザベースの防御の有効性について、縦断的かつ定量的な分析を行いました。[49]

そして以下の 3 つの質問に答えるように試みました。

1. 主要なブラウザはどのようなポリシーを実装し、それらのポリシーをどの程度適切に実施しているのか?
2. 2.既存のポリシーを体系的に回避する方法があるのか?
3. Web サーファーは IDN ホモグラフをどの程度認識でき、また、ブラウザのポリシーを回避する IDN ホモグラフに大体は騙されるものなのか?

これらの質問に答えるために、著者らは 5 年間 (2015 年 1 月から 2020 年 4 月まで) に渡って 5 つの主流ブラウザ (Chrome、Firefox、Safari、Microsoft Edge、Internet Explorer) を調査しました。最初の 2 つの質問に答えるために 9,000 件のテストケースを生成し、3 番目の質問に答えるためにユーザ調査を実行しました。Chrome と Edge は、対応する IDN ホモグラフの代わりに Punycode を表示することに最も成功しました。両方のブラウザの全体的な失敗率 (Punycode の代わりに IDN バージョンを表示) は 20.62% でした。Safari と Firefox はもっとひどく、全体的な失敗率はそれぞれ 42.91% と 44.46% でした。各ブラウザでは、IDN のカテゴリにより失敗率が異なりました。さらに、著者らは、Web サーファーがホモグラフの IDN を識別するのに苦労していること、そして、ブラウザがブロックしている IDN は、ユーザの 48.8 % が本当のものだと思い、48.5 % は偽物だと思い、2.7 % はどうとも言えないと、真偽を判断する上で最も厄介であることを発見しました。

ここまでは、デスクトップブラウザのみに焦点を当ててきました。しかし、本レポートで前述した類似ドメイン スミッシング攻撃で見てきたように、IDN ホモグラフドメインはモバイルデバイスでも非常に馴染み深いものです。それどころか、もっと悪質なのかもしれません。画面サイズが小さく、アドレスバーも小さく、リンクプレビューが通常不足しているために、より効果的な Lookalike domain 攻撃につながる可能性があります。リンクプレビューがある場合でも、IDN ホモグラフはモバイルデバイスで効果的です。2021 年に、セキュリティ研究者の Tyler Butler 氏は、iMessage で IDN ホモグラフを使用してスミッシングの妥当性について発表しました。[50] iMessage はリンクのリッチプレビューを提供しますが、巧妙な攻撃者は、十分に類似したドメインと Web ページ自体の形式に少し手を加えて、これを非常に簡単に回避できます。Butler 氏が指摘しているように、この形態の攻撃は、誤った情報の拡散、認証情報の盗用、標的型マルウェアやスパイウェアの配信に使用される可能性があります。

Butler 氏は、Apple はホモグラフは「視覚的に区別できる」ことを理由に、この脆弱性に対処しないと主張していると述べています。図 22 を見て、どう思いますか?違いを見つけることができますか?

間違いを犯すのは人間であり、許すのは神 ...
しかし自動化は賢明な選択

ワールドワイドウェブ上には、人間はいないために、他人の間違いは許されます。
でに述べたように、攻撃アクターはタイポスクワットドメインを使用して他の人たちの自然な間違いを餌食にします。タイポスクワットを有効にするためにすべての攻撃者がしなければならないことは、もっともらしいドメインを登録して待つだけです。それだけです。遅かれ早かれ、人間はスペルミスを犯し、訪れるつもりのなかったドメインに着陸します。もちろん、悪意のある攻撃者はただ待っているだけではなく、積極的にユーザをクリックするよう誘導します。そして、現在の目まぐるしく動き続ける世界では、多くの場合、ミスを犯したことさえ気がつきません。

結局のところ、類似ドメインが類似ドメインと呼ばれるのには理由があります。人間を欺く目的で既知のドメインに似ているからです。
これまで見てきたように、一部の類似ドメインは他の類似ドメインよりも効果的ですが、ドメイン名の選択は類似ドメインの有効性の一部にすぎません。類似ドメインの展開方法も、組織的な活動の全体的な成功に大きな影響を与える可能性があります。例えば、okta[.] Infoblox[.]com、または okta-Infoblox[.]com のような Okta または MFA の類似ドメインを見ていきます。注意深い人は、訪問する前に各ドメイン名をトリプルチェックして (そのような人たちが見つけることができるよう幸運を祈る)、第 2 レベルドメイン (SLD) の「i」が実際には小文字の「L」であることに気付くかもしれません。しかし、その類似ドメインと、例えば、雇用主のオンラインプロフィールに登録されている電話番号への巧妙な SMS メッセージが組み合わされると、違いを生む可能性があります。これに緊急の行動喚起を伴う電話まであると、そこまでです。もちろん、これはすべての構成要素を使用しているスピアフィッシングの架空の例であり、類似ドメインを使用している一般的な組織的活動ではありませんが、重要な点は、類似技術が複数の方法でドメインに、DNS インフラストラクチャの複数の部分に効果的に適用できるということです。

これらはすべて、よく引用される「一度だけ私を騙したら、君の恥。二度も私を騙したら、私の恥。」ということわざは、類似ドメインには当てはまりません。非常に厳しい目を持ち、セキュリティ意識の高い人でも、類似ドメインの餌食になる可能性があり、何度もそれを繰り返してしまいます。この戦いでは悪意のある攻撃者が優位に立っていますが、それで負けではありません。Infoblox は、組織が反撃して効果的に防御できるようにするための DNS レベルのソリューションを備えています。

IOCs 

本レポートの全リストは *GitHub* のこちらから
https://github.com/infobloxopen/threat-intelligence

INFOBLOX ソリューション

類似ドメインは、その有効性と大規模な検出の難しさから、依然として攻撃者に人気があります。正当なターゲットを模倣することを目的とした疑わしいドメインを自動的に識別することが難しいため、この課題はさらに複雑になります。その結果、企業や政府機関は、企業ドメインやサプライチェーンになりすました、類似ドメインに対する懸念をますます強めています。

Infoblox BloxOne Threat Defense（B1TD）Advanced は、Looka like 攻撃の脅威に対して独自の広範かつ包括的なソリューションを提供します。大規模に DNS を活用することで、Infoblox は毎日数十万の新しい SLD に対して一連の分析を適用できます。これには、IDN ホモグラフの視覚的類似性の自動評価など、類似検出のための複数の分析が含まれます。

お客様は、一般的にターゲットにされたドメインから選択するか、独自に類似の監視と分析のためのカスタムリストを作成できます。この詳細な分析の結果は類似ドメインレポート UI（不審な活動やフィッシングが疑われる活動に関連している、類似ドメインが検出された場合にはフラグも立てます）からアクセスできます。全体として、ポリシーは、お客様特有の環境のニーズとリスク許容度のレベルに合わせてカスタマイズできます。また、詳細なドメインデータには、B1TD Advanced UI および API からアクセスできる貴重な注釈が含まれ、脅威調査を迅速化し、インシデント対応をより効果的にするためのコンテキストをお客様に提供します。

これらの類似脅威検出機能は、BloxOne Threat Defense が提供する多くのサービスの 1 つに過ぎず、他のソリューションでは認識できない脅威を認識し、脅威のライフサイクルの早い段階で攻撃を阻止できるようになります。広範囲の自動化とエコシステムの統合を通して、SecOps の効率は推進され、既存のセキュリティスタックの有効性が向上し、デジタル化とどこからでも作業できる取り組みが安全になると共に、サイバーセキュリティのための総コストが削減されます。

詳細については

infoblox.com
をご覧ください。

Follow-us on LinkedIn

Follow-us on Twitter

参考文献

[1] https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf

[2] https://twitter.com/kgroupcompanies/status/1188878363068391425

[3] https://en.wikipedia.org/wiki/IDN_homograph_attack

[4] https://i.imgur.com/68oL4U9.jpg

[5] https://www.researchgate.net/publication/220420915_The_Homograph_Attack

[6] https://util.unicode.org/UnicodeJsps/confusables.jsp

[7] https://www.igoldrush.com/domain-guide/domain-legal-issues/cybersquatting-and-typosquatting

[8] https://dl.acm.org/doi/pdf/10.1145/3133956.3134002

[9] https://core.ac.uk/download/pdf/34615371.pdf

[10] https://iris.polito.it/retrieve/handle/11583/2970511/1dd2efbb-9eed-4db5-be4f-ecfcc362572c/_Workshop__Data_driven_Soundsquatting_Generation%20(7).pdf

[11] https://incolumitas.com/2016/06/08/typosquatting-package-managers/

[12] https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

[13] https://www.akamai.com/blog/security-research/combosquatting-keyword-analysis-support

[14] https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/c/iron-tiger-sysupdate- reappears-adds-linux-targeting/IOCs-iron-tiger-sysupdate-reappears-adds-linux-targeting.txt

[15] https://urlscan.io/result/41e8b29f-55cc-4887-9186-41a064ffb2ac/

[16] https://thehackernews.com/2022/07/microsoft-warns-of-large-scale-aitm.html

[17] https://thehackernews.com/2023/03/microsoft-warns-of-large-scale-use-of.html

[18] https://www.hackread.com/hackers-employee-accounts-twilio-internal-system/

[19] https://www.feldmanauto.com/

[20] https://urlscan.io/result/98f407d6-96b4-4652-bd38-aa44470b5b78/

[21] https://urlscan.io/result/98f407d6-96b4-4652-bd38-aa44470b5b78/

[22] https://blogs.infoblox.com/cyber-threat-intelligence/scammers-first-on-the-scene-for-turkiyes-disaster-of-the-century/

[23] https://urlscan.io/result/4f295f57-7d46-49e9-94f6-d90858a4cfeb/

[24] https://www.coindesk.com/web3/2023/03/02/nft-trading-volumes-hit-2b-in-february-highest-since-luna-crash-thanks-to-blur/

[25] https://nftnow.com/guides/blurs-token-just-dropped-heres-what-you-need-to-know/

[26] https://twitter.com/blur_io/status/1630290782211981312/

[27] https://www.wired.com/story/youtube-bitcoin-scam-account-hijacking-google-phishing/

[28] https://twitter.com/FoolishBB/status/1627059614654279682

[29] https://www.bleepingcomputer.com/news/security/fake-crypto-giveaways-steal-millions-using-elon-musk-ark-invest-video/

[30] https://www.domaintools.com/

[31] https://urlscan.io/result/8e94bf31-7295-47e8-9de4-756743937f46/

[32] https://www.domaintools.com/

[33] https://urlscan.io/result/7f3c8f83-1922-4570-a9b1-1542e32ccc89/

[34] https://urlscan.io/result/f60f5548-4b54-4a97-add5-1f37a89f4e7e/#summary

[35] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a

[36] https://blogs.infoblox.com/cyber-threat-intelligence/cyber-campaign-briefs/dont-dial-that-number-distribution-of-phishing-lookalikes-through-fake-support-calls/

[37] https://urlscan.io/result/41a6ef99-fef1-4d08-80e1-623123280b6a/

[38] https://walletconnect.com/

[39] https://urlscan.io/result/a79ba8e3-9f9a-4a9c-b54b-b26a300afc23/

[40] https://bitkeep.com/

[41] https://docs.flutter.dev/

[42] https://www.welivesecurity.com/2023/02/16/these-arent-apps-youre-looking-for-fake-installers/

[43] https://www.virustotal.com/gui/file/ 271229d5d007baf5324fb2705b7a0b3751bd228bbdb08a86e7b7e2856bbf9b08

[44] https://urlquery.net/report/ef86060b-39e3-4e41-a480-a2b138ee0a49

[45] https://elifesciences.org/articles/54846

[46] https://chromium.googlesource.com/chromium/src/+/main/docs/idn.md

[47] https://wiki.mozilla.org/IDN_Display_Algorithm

[48] https://www.xudongz.com/blog/2017/idn-phishing/

[49] https://www.usenix.org/system/files/sec21-hu-hang.pdf

[50] https://tbutler.org/2021/04/16/considering-the-plausibility-of-idn-homograph-attacks

Infoblox はネットワークとセキュリティを統合して、比類の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、脅威を早期に検知・対処できます。

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