infoblox

Threat Intel

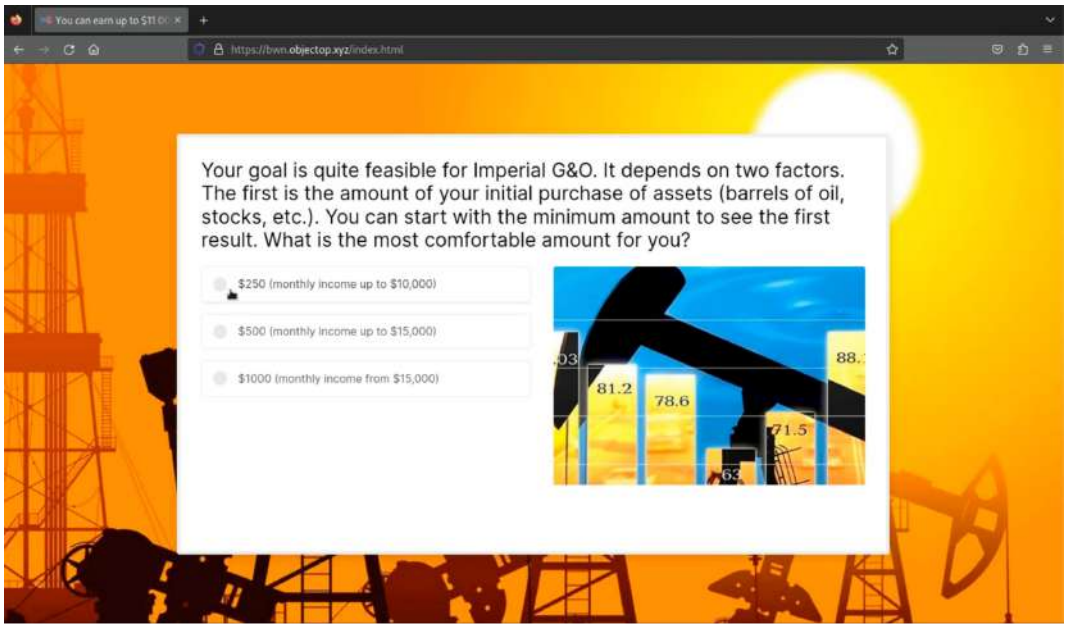
FACEBOOK 広告を通じて 偽投資プラットフォームへ誘導

著者：
Stelios Chatzistogias
Laura da Rocha
Darby Wise

目次

エグゼクティブサマリー

DNS 脅威アクターは、私たちを驚かせ続けます。新しい攻撃手法の開発や被害者を標的にした創造的なキャンペーンについて、私たちは日々学び続けています。投資詐欺もその中の一つです。米国連邦取引委員会の報告によると、2023 年に米国で投資詐欺によって失われたお金は他のどのタイプの詐欺よりも多く、被害金額は合計で46 億米ドルを超えました。[1] Savvy Seahorse は、被害者を説得して偽の投資プラットフォームでアカウントの作成、個人アカウントへの入金、その入金をロシアの銀行へ送金と誘導する DNS 脅威アクターです。このアクターは Facebook 広告を使ってユーザーをウェブサイトに誘導し、最終的には偽の投資プラットフォームに登録させます。キャンペーンのテーマには、Tesla、Facebook/Meta、Imperial Oil などの有名企業へのなりすましが含まれることがよくあります。



Savvy Seahorse のキャンペーンは洗練されています。これらのキャンペーンには、ユーザーに自動応答を提供し、高収益の投資機会と引き換えに個人情報を入力するよう促す偽の ChatGPT や WhatsApp ボットを組み込むなど高度な手法が含まれています。これらのキャンペーンは、ロシア語、ポーランド語、イタリア語、ドイツ語、チェコ語、トルコ語、フランス語、スペイン語、英語圏の人々をターゲットにしていることが知られ、特にウクライナやその他の少数の国の潜在的な被害者は保護されるようになっています。

Savvy Seahorse は、Domain Name System（DNS）を目立たない方法で悪用します。DNS の正規名（CNAME）レコードを利用して、高度な金融詐欺キャンペーンのためのトラフィック分散システム（TDS）を構築しています。その結果、Savvy Seahorse はコンテンツにアクセスできるユーザーを制御でき、悪意のあるキャンペーンの IP アドレスを動的に更新できるようになります。CNAME を使用するこの手法により、脅威アクターはセキュリティ業界による検出を回避できました。私たちの知る限り、これは悪意のある目的で設計された TDS としての CNAME の使用に焦点を当てた最初のレポートです。

このホワイトペーパーでは、CNAME TDS の概念を紹介し、Savvy Seahorse が CNAME レコードを使用して、これまでセキュリティ業界の監視を水面下で逃れてきた大規模な詐欺キャンペーンをどのように実行しているかについて説明します。主な調査結果は次のとおりです。

1 https://www.ftc.gov/business-guidance/blog/2024/02/facts-about-fraud-ftc-what-it-means-your-business

- Savvy Seahorse は Facebook 広告を通じてキャンペーンを実施します。
- Savvy Seahorse は少なくとも 2021 年 8 月から運営されています。
- 専用ホスティングを使用し、IP アドレスを定期的に変更しています。
- 個々のキャンペーンは短期間です（各サブドメインは 5〜10 日間宣伝されます）。
- キャンペーンドメインの CNAME レコードが現在アクティブかどうかによって変わる段階的な展開システムを使用しているようです。
- ワイルドカード DNS エントリを利用しているため、多数の独立したキャンペーンを迅速に作成できますが、パッシブDNS（pDNS）分析には混乱を招く可能性があります。
- 被害者の個人データは、情報を検証し、ウクライナと他のいくつかの国を除外するためのジオフェンシングを適用するために、セカンダリ HTTP ベースの TDS サーバーに送信されます。
- 2 番目の HTTP ベースの TDS も、時間の経過に伴ってユーザーの IP とメールアドレスを追跡します。

用語の使い方について

DNS に関連する RFC（Request For Comment）文書は数百に上り、ネットワーク分野以外のセキュリティ業界が DNS 用語を使用する方法と組み合わせると、特に用語について混乱が生じ、矛盾が生じる可能性があります。このホワイトペーパーで使用する DNS 用語は次のとおりです。

- **ドメイン名とは**、DNS レコードに割り当てられた完全修飾ドメイン名（FQDN）を指します。www[.]infoblox[.]com と infoblox[.]com はどちらもドメイン名です。FQDN、ドメイン名、ドメインは同じ意味で使用されます。
- **ベースドメイン**は、ドメイン名またはサブドメインに関連付けられたセカンドレベルドメイン（SLD）になります。たとえば、www[.]infoblox[.]com および blogs[.]infoblox[.]com のベースドメインは infoblox[.]com です。ベースドメインは、登録されたドメインと考えることができます。
- **サブドメイン**は、別のドメイン内に適切に存在しているドメインを指します。したがって、www[.]infoblox[.]com と blogs[.]infoblox[.]com は infoblox[.]com のサブドメインです。DNS 管理者はうんざりするでしょうが、この用語を理解することで脅威インテリジェンスの読者にとって理解しやすいものになります。
- **ホスト名**は、ドメインの一番左のラベルを指します（例：www）。
- **CNAME ドメイン**は、正規ドメイン名（CNAME）レコードのドメイン名の値です。
- この場合の**キャンペーンドメイン**は、Facebook 広告から被害者を誘導するために使用されるドメインです。

DNS の CNAME レコード

DNS の CNAME レコードは、ドメイン名のエイリアスを作成するメカニズムを提供します。これらのレコードは幅広い目的で使用され、DNS 構成管理をより簡単かつ堅牢にすることを目的としていて、DNS レコードの総数が削減され、IP アドレスの切り替えが容易になります。CNAME レコードの典型的な使用例は、Web ページに使用されるサブドメインをベースドメインにマッピングすることです。

たとえば、ほとんどの Web サイトでは、ホスト名として www が使用されています。www.infoblox.com の FQDN には、infoblox.com の値を持つ CNAME レコードがある場合があります。この場合、クライアントが www.infoblox.com の IP アドレスをクエリすると、infoblox.com の IP アドレスが返されます。再帰リゾルバがユーザーに代わって解決を処理するため、CNAME の存在はユーザーにはほとんど見えません。[2]www.infoblox.com は infoblox.com のエイリアスであると言えます。

2 https://datatracker.ietf.org/doc/html/rfc1034#section-4.3.2

図 1 に示すように、解決までの一連のイベントは、おおよそ次のようになります。

- スタブリゾルバであるクライアントは、www.infoblox.com について再帰リゾルバに照会します。
- 再帰リゾルバは、www.infoblox.com の IP アドレス（A レコード）を DNS にクエリし、応答として infoblox.com を含む CNAME レコードを受け取ります。
- 再帰リゾルバは、infoblox.com の IP アドレスを DNS にクエリします。[3]
- 再帰リゾルバは、CNAME レコードとともに IP アドレスをクライアントに返します。
- 最後に、クライアントサービス（ブラウザーなど）が提供された IP アドレスに接続します。

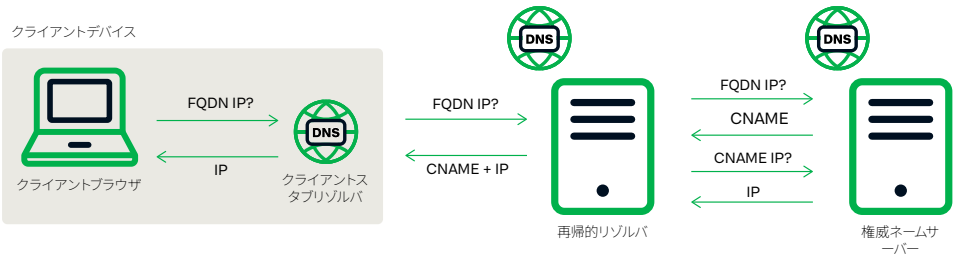


図 1：完全修飾ドメイン名の *DNS CNAME* レコードがある場合の *IP* アドレス解決の簡略図。

この場合の DNS ゾーンファイルのレコードには次の内容が含まれる可能性があります。

FQDN	レコードタイプ	価値
www.infoblox.com	CNAME	infoblox.com
infoblox.com	A	127.0.0.1

レコードの左側は、正規のドメイン名の**エイリアス**と言われています。つまり、www.infoblox[.]com は infoblox[.]com のエイリアスです。www[.]infoblox[.]com と infoblox[.]com の両方の A レコードをクエリすると、127.0.0.1 が返されます。正規ドメイン名、つまり CNAME レコードの値は、FQDN である必要があります。

CNAMEトラフィック分散システム

CNAME レコードの典型的な使用例は、www ホスト名をベースドメインにマッピングすることですが、実際にはさまざまな方法で使用されています。CNAME レコードは、多くのコンテンツ配信ネットワーク（CDN）で使用されています。上記の例では、www[.]infoblox[.]com が infoblox[.]com のエイリアスである可能性があると示唆しましたが、実際にはそうではありません。Infoblox は、今日のほとんどの主要企業と同様に、商用 CDN プロバイダーを使用しています。実際には、www[.]infoblox[.]com には、CDN プロバイダー内に CNAME ドメインがあります。CDN の主な目的は、世界中のユーザーがどこにいても Web サイトのコンテンツに高速にアクセスできるようにすることです。このアクセスを実現するために、CDN プロバイダーは、キャッシュやプロキシのアプライアンスなどの高度なホスティング環境を使用することが多いですが、これらのメカニズムはすべて DNS 構成から独立しています。

TDS は、インターネットトラフィックのソースを宛先に接続します。この用語は、TDS が Web サイト訪問者を広告に接続するインターネットマーケティングから生まれました。悪意のあるハッカーはこの手法を利用して、合法的なマーケティング目的で使用される TDS の概念をサイバー犯罪活動に使用できるように変更しています。Infoblox では、DNS のみに基づき、要求者の IP アドレスのみに基づ

3 CNAME 値を解決する責任はスタブリゾルバにあるという言い方がありますが、ほとんどの再帰的リゾルバは自動的に解決プロセスを完了し、組み合わせた応答を返します。

いて決定を下すシステムなど、TDS を作成するために使用されるさまざまな手法を確認しています。VexTrio や[4]Prolific Puma に関する以前の出版物では、[5]悪意のある TDS の複数の例について説明しました。VexTrio は DNS TDS と HTTP ベースの TDS の両方を運営し、Prolific Puma はリンク短縮サービスを運営しています。正当なマーケティング TDS は、あらゆるユーザーを関連する広告コンテンツに誘導することを目的としていますが、悪意のある TDS にはトラフィック制御も組み込まれいて、特定のユーザーが実際のコンテンツにアクセスできないように制限することがあります。悪意のあるキャンペーンの中には、複数の TDS を連鎖させるものもあります。

Savvy Seahorse は、悪意のある TDS の一部として DNS CNAME を悪用する脅威アクターとして初めて公に報告されました。脅威アクター側には DNS に関するより高度な知識が要求されますが、セキュリティに関する文献ではこれまで認識されていなかっただけで、珍しいことではありません。私たちは **CNAME TDS** という用語を使って、DNS の CNAME レコードを使って TDS を作成する手法を説明します。しかし、CDN とは異なり、TDS はすべてのユーザに同じコンテンツへの平等でパフォーマンスの高いアクセスを提供するようには設計されていません。

DNS CNAME レコードを使用して不正な活動の TDS を作成するというのは、脅威アクターにとっては新しい概念ではないかもしれませんが、セキュリティ業界では新しいもののようです。少なくとも 2021 年以来、Savvy Seahorse はこれまで報告されていなかったこの手法を利用してインフラストラクチャを構築し、投資先を探している Facebook/Meta ユーザーをターゲットにした詐欺キャンペーンを実施してきました。私たちは、CNAME 技術のバリエーションを使用する他の多くの攻撃者も追跡しています。

CNAME から SeaNAME へ

Savvy Seahorse は、CNAME のドメイン置換メカニズムを採用し、主要なキャンペーンドメインに関連付けられた特定のサブドメインを作成します。特に、悪意のあるキャンペーンドメインはすべて、次のサブドメインのエイリアスです。

`b36cname[.]site`

たとえば、Savvy Seahorse は以前、Mastercard 投資プログラムを偽装するキャンペーンで、`mom[.]multi-info[.]site` ドメインを使用していました。このドメインには、`prx16[.]b36cname[.]site` という値を含む CNAME レコードがありました。同時に、攻撃アクターはキャンペーンで `multi-info[.]site` の他の多くのサブドメインを使用していました。Savvy Seahorse はワイルドカード DNS 構成を使用しているため、これらすべてが同じ IP アドレスを共有していました。図 2 にこの構成を示します。

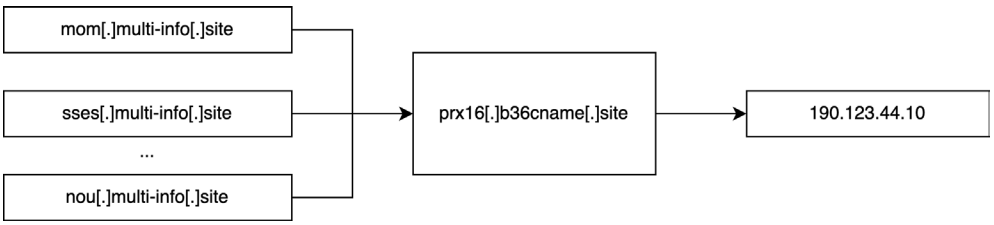


図 2：*Savvy Seahorse* は、同じベースドメインのサブドメインである多くのキャンペーンドメインを同時に使用しています。これらのサブドメインでは *CNAME* レコードが共有され、*IP* アドレスも共有されています。

Savvy Seahorse は、コンテンツをホストするために専用の IP アドレスを使用しています。CNAME を使用すると簡単にローテーションできるため、DNS 海域での検出や偽装を回避できるように、アクターはこれらの IPアドレスを定期的にローテーションしています。

4 https://blogs.infoblox.com/cyber-threat-intelligence/cybercrime-central-vextrio-operates-massive-criminal-affiliate-program

5 https://blogs.infoblox.com/cyber-threat-intelligence/prolific-puma-shadowy-link-shortening-service-enables-cybercrime/

Savvy Seahorse のキャンペーンドメインには簡単に区別できるパターンがなく、ホスティングのインフラストラクチャも大幅に異なる可能性があります。これについては、後のセクションでさらに詳しく説明します。これらのバリエーションにより、脅威研究者がアクティビティを単一の DNS 脅威アクターから発生したものとして特定することがより困難になる可能性があります。最終的に、このネットワークを結び付けることができた唯一の情報は、共通の CNAME の使用でした。

SAVVY SEAHORSE の運営

Savvy Seahorse は、b36cname[.]site ドメインが最初に作成された 2021 年 8 月から運営されています。参加しているドメインはセキュリティツールによってフラグが付けられることもありますが、その背後にある大規模なインフラストラクチャとアクターはセキュリティ業界によって検出されていません。私たちは、サブドメインの b36cname[.]site をリストしている CNAME レコードを持つ約 4.2k のベースドメインを確認しました。キャンペーンをホストするために、Savvy Seahorse はドメイン生成アルゴリズム（DGA）を使用して各 SLD に複数のサブドメインを作成しています。ホスト名は疑似ランダムで、ほとんどの場合 3 文字の長さです。次のセクションでは、このホスト名パターンについて詳しく説明します。

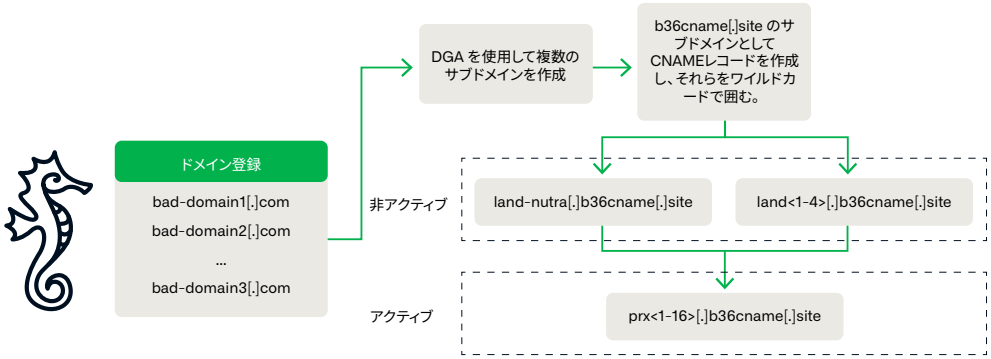


図 3：*Savvy Seahorse* の運営概要

SeaNAME パターンとワイルドカード

Savvy Seahorse の CNAME レコードはそれぞれ、表 1 に示しているような次の 3 つのパターンのいずれかに該当します。

CNAME パターン	目的
land-nutra[.]b36cname[.]site	キャンペーンがアクティブになる前のパークドメインの CNAME として一時的に使用されたサブドメイン
land<1-4>[.]b36cname[.]site	キャンペーンがアクティブになる前のテスト目的などで一時的に CNAME として使用されたサブドメイン
prx<1-16>[.]b36cname[.]site	アクティブなキャンペーンに使用されるサブドメイン

表 1：*CNAME* レコードのパターンと目的

以下は、Savvy Seahorse の各タイプの CNAME の使用時に観察された動作です。

その間、CNAME レコードとして land-nutra[.]b36cname[.]site を持つドメインは使用されていませんでした。キャンペーンがアクティブになると、攻撃者は CNAME レコードを prx<1-16>[.]b36cname[.]site に変更しました。

同様に、ある時点で <1-4>land[.]b36cname[.]site を CNAME レコードとして持っていたドメインは、非アクティブなキャンペーンに使用されていました。これらのドメインも、キャンペーンがアクティブになったときに prx<1-16>[.]b36cname[.]site レコードに変更されました。

land<1-4> CNAME は、一部のキャンペーンを有効にする前にテストするために使用された可能性があります。[6]

Savvy Seahorse は、DNS の使用を簡単に管理できるように、ワイルドカード CNAME 応答を構成しています。この場合、ベースドメインの任意のサブドメイン（ wildcard[.]xsdelx[.]top など）へのクエリは、同じリソースレコードを共有していることを示す応答を返します。図 4 は、dig コマンドを実行して xsdelx[.]top Savvy Seahorse ベースドメインの wildcard[.]xsdelx[.]top をクエリした結果を示しています。この応答は、ワイルドカードの結果として、クエリが CNAME レコード prx2[.]b36cname[.]site を返したことを示しています。ワイルドカードを使用すると、攻撃者は作成する新しいサブドメインのレコードを自動的に設定できるため、大規模なインフラストラクチャをより効率的に管理できます。

```
; <<>> DiG 9.10.6 <<>> +trace wildcard.xsdelx.top
;; global options: +cmd
.                       3328    IN      NS      b.root-servers.net.
.                       3328    IN      NS      g.root-servers.net.
.                       3328    IN      NS      d.root-servers.net.
.                       3328    IN      NS      f.root-servers.net.
.                       3328    IN      NS      e.root-servers.net.
.                       3328    IN      NS      i.root-servers.net.
.                       3328    IN      NS      m.root-servers.net.
.                       3328    IN      NS      a.root-servers.net.
.                       3328    IN      NS      h.root-servers.net.
.                       3328    IN      NS      c.root-servers.net.
.                       3328    IN      NS      j.root-servers.net.
.                       3328    IN      NS      k.root-servers.net.
.                       3328    IN      NS      l.root-servers.net.
.                       3328    IN      RRSIG   NS 8 0 518400 20240124220000 20240111210000 30903 . KAZZGJQ19L65se3m2Evl4S/ucf
SV7rPzcTEXZvIiTa96qIyXNdw5+L5R Ece44fVVTc7Kpr2UK844Zb9qnGcjiB22XHqWoeYjyRZgQ2kuEHkVVTC+ jLNeRqQQ84cleKWPebpiSo73paJE3iLqpug8fR
9DUzbW4+XmNFW1lNak ahTafUnmBDbe7fJ/AkI9lH2PdqSTrB882vGZI/UYfBWG38E5mslTS/aa NAL2yIsGYCuargdZDGkp9yOa6q2khrjBBNUeqhlrOQU63yh+qF
rzJ851 O7iyiQmXwl2j22vEzncv23ue16CgHIUu2yaJLGmxI5m9N2lBHAPvgzlC zpdGZg==
;; Received 717 bytes from 127.0.0.2#53(127.0.0.2) in 57 ms

top.                    172800  IN      NS      a.zdnscloud.com.
top.                    172800  IN      NS      b.zdnscloud.com.
top.                    172800  IN      NS      c.zdnscloud.com.
top.                    172800  IN      NS      d.zdnscloud.com.
top.                    172800  IN      NS      f.zdnscloud.com.
top.                    172800  IN      NS      g.zdnscloud.com.
top.                    172800  IN      NS      i.zdnscloud.com.
top.                    172800  IN      NS      j.zdnscloud.com.
top.                    86400   IN      DS      56384 8 2 BA378C5913404EC654DF544F519B0FB287E140D64DAC5D59E3499623 93C17945
top.                    86400   IN      RRSIG   DS 8 1 86400 20240124220000 20240111210000 30903 . z+m6M/ORJDt+eyaQ/jjqUr9G5b+
fosBjAsw5MKrYyGbIjNaYQoBDBtvi bZsVI7YD3vAlRf7Hf1eOavQJ8nC57B3dsED4jKJ32ulMsHNxJ/+7Nbf/ XZMc20886b6FQC/LxUxYFFw4+fTrfJX1ydp4Ze2
gJi2amF3hWEQJO6aW bP+NiAiT4UTW74AMZH31BLhtYDHkVKzHjXGSGcgBn9Zp4mesaf/fjxQK o3QCgmD8Kb7sqmULt4RMirZUxEYrbHC/LO+GsPb9aAcKA5qC2/8
/if3s j/q4wh5NlD5Asdai2cGhd2oY1JMGBmLVBgEWMIAONBiPSWTR2JimteSe 42BWyQ==
;; Received 676 bytes from 2001:500:2d::d#53(d.root-servers.net) in 24 ms

xsdelx.top.             3600    IN      NS      ns1.dns.com.
xsdelx.top.             3600    IN      NS      ns2.dns.com.
nmb1kc8kpr7nahib8f3qbcm0q3q4s611.top. 3600 IN NSEC3 1 0 0 - NMB1KT4CELS35EVJ7GVFSKCJB2HGKQGA  NS
nmb1kc8kpr7nahib8f3qbcm0q3q4s611.top. 3600 IN RRSIG NSEC3 8 2 3600 20240119124502 20240105021522 9610 top. b8QG+wOZ+V9gRsl8/ty
UoISU9cTbU3Ha6mh7O/SyeInAtGX9KG2Kl+nU g3RoIofAm6A2GoQmOiQ5hzLPWYPjelSjLXE1PJBUAIYknGxToHz55RE8 JRLb/e4FqZphjgB6EicSKazMW1HA2co
v49hq/lWLzTtg/LduzXQmOAWZ 9SE=
;; Received 331 bytes from 2401:8d00:2::1#53(j.zdnscloud.com) in 166 ms

wildcard.xsdelx.top.    600     IN      CNAME   prx2.b36cname.site.
xsdelx.top.             86400   IN      NS      ns1.dns.com.
xsdelx.top.             86400   IN      NS      ns2.dns.com.
;; Received 130 bytes from 183.253.57.193#53(ns2.dns.com) in 256 ms
```

図 4：既存の *Savvy Seahorse* ベースドメインのランダムなサブドメインに対するワイルドカード応答の動作。サーバーはサブドメインに応答し、そのサブドメインに、攻撃者の *CNAME* ドメインである prx2[.]b36cname[.]site の *CNAME* レコード値があることを示していました。

ドメイン

脅威アクターは、キャンペーンの運営やその他の悪意のある活動に使用できる疑似ランダムドメイン名を大量に生成するツールとして DGA をよく使用します。これらの DGA で使用されるドメインは、専用のアルゴリズムが容易に検出でき、それによって脅威アクターとの相関を容易にすることができる、目に見える類似のパターンに従うことがよくあります。Savvy Seahorse は多くの SLD とサブドメインを作成するために DGA を使用しているようですが、これらの DGA は 1 つの明確なパターンに従っているようには見えません。むしろ、表 2 に示すように、攻撃者が SLD に複数の DGA パターンを使用しているのが観察されました。

6 https://urlscan.io/result/f6521352-dc51-4352-9d5f-691268e17c8c/

パターンの説明	同じ完全なキーワードのバリエーション	同じ長さのランダムな文字が追加された完全なキーワード	キーワードの後半のスペルのバリエーション	ドメイン全体でのキーワードのバリエーション
サンプルドメイン	program-delo[.]site program-lid[.]site program-lids[.]site program-life[.]xyz program-plus[.]site program-plus[.]xyz program-pro2[.]xyz program-world[.]site programbndr[.]site programerstr[.]xyz programfuture[.]site programinject07[.]site programir[.]xyz programm-one[.]site programs-pl[.]site	formaa[.]top formew[.]top formhh[.]top formpr[.]top	anticriss-es[.]xyz anticrisses[.]xyz anticriz[.]site anticrsss-ep[.]xyz anticrsss1-ep[.]xyz anticrys[.]xyz anticrysz[.]site antikrys[.]xyz	zol0to-rus[.]xyz zolotoru[.]site xoloto-ru[.]xyz zolotoros[.]site

表 2：*Savvy Seahorse SLD* パターンとドメインの例

これらのタイプの DGA を識別するための一般的な手法は、機械学習アルゴリズムを使用することです。N-gram を使用して[7]表 2 の各列のクラスターの一部を正常に検出することもできますが、その方法では、ドメインラベルの特徴だけを見ても、これらすべてのクラスターが単一の DNS 脅威アクターに属していることを検出できません。上記の 4 つのクラスターはすべて、Savvy Seahorse が作成する他のドメインクラスターと同様に非常に異なるパターンを持っているため、N-gram ベースのモデルでは、同じグループに属していると検出できません。

上記の例は、攻撃者が、異なる DGA 命名パターン内であっても、1 つのトップレベルドメイン（TLD）だけに固執していないことも示しています。Savvy Seahorse は複数の TLD を使用し、その多くは悪用されていることで知られているものです。ドメイン数による上位 5 つは、site、`xyz`、`com`、`top`、`life` です。

7 https://en.wikipedia.org/wiki/N-gram

TLD	サイト	xyz	com	トップ	life
ドメイン	imsol[.]site lareg[.]site mstpr[.]site tayki[.]site teraw[.]site	newtrds[.]xyz newtrdin[.]xyz newstrdinfo[.]xyz newstrdinfos[.]xyz	gelopro[.]com welerpro[.]com glowtrad[.]com strprogram[.]com	newlvlpro[.]top newplatf[.]top newplattf[.]top newplf[.]top newprogf[.]top gelopro[.]com welerpro[.]com glowtrad[.]com strprogram[.]com	maxhongtrade[.]life firehongtrade[.]life librahongtrade[.]life

表3：*Savvy Seahorse* の悪意あるキャンペーンで最もよく使用される *TLD* のサンプルドメイン

以前、ホスト名はほとんどの場合擬似ランダムで3文字の長さに見えると言いましたが、ラベルが長い例もいくつか見てきました（表 4 を参照）。

byseniscon[.]top	worldtrades[.]top	tesxprofit[.]top
per[.]byseniscon[.]top	bln[.]worldtrades[.]top	bkz[.]tesxprofit[.]top
bzmm[.]byseniscon[.]top	bts[.]worldtrades[.]top	gfk[.]tesxprofit[.]top
i9us[.]byseniscon[.]top	cai[.]worldtrades[.]top	krx[.]tesxprofit[.]top
ijks[.]byseniscon[.]top	cpq[.]worldtrades[.]top	kvn[.]tesxprofit[.]top
ji8s[.]byseniscon[.]top	da2[.]worldtrades[.]top	mcr[.]tesxprofit[.]top
q89k[.]byseniscon[.]top	dab[.]worldtrades[.]top	mld[.]tesxprofit[.]top
u76a[.]byseniscon[.]top	dha[.]worldtrades[.]top	ndx[.]tesxprofit[.]top
jskks[.]byseniscon[.]top	dl5[.]worldtrades[.]top	nfk[.]tesxprofit[.]top
nbxnz[.]byseniscon[.]top	ewt[.]worldtrades[.]top	nqs[.]tesxprofit[.]top
nuuvi[.]byseniscon[.]top	fe0[.]worldtrades[.]top	nzb[.]tesxprofit[.]top

表 4：サブドメインパターンの例

登録情報

Savvy Seahorse は検出を回避できるように登録の処理方法に従来のアプローチを採用していません。DNS の脅威アクターが使用する一般的な手法は、同じレジストラを通じてドメインを一括登録し、同じインターネットサービスプロバイダー（ISP）を使用してドメインをホストすることです。これにより、インフラストラクチャをより簡単かつ迅速に管理できます。多くのレジストラは、ドメインの一括登録を容易にする API を提供しています。ほとんどのレジストラは API が正当な目的で使用されることを想定していますが、サイバー犯罪者はこの機能を悪用して、キャンペーンに使用する何千ものドメインをより簡単に作成することで知られています。2023 年 10 月の RDGA に関するブログでは、このプロセスについてさらに詳しく説明しています。[8]

アクターが同じレジストラとインフラストラクチャを利用してドメインを作成し、ホストする場合、共通の登録メタデータを通じて同じアクターに属するドメインを見つけるのは簡単です。Savvy Seahorse は、インフラストラクチャが複数の異なるレジストラとホスティングプロバイダーに分散している、より忍耐強い生き物のようです。私たちは、CNAME レコードとして `b36cname[.]site` のサブドメインを持つすべてのドメインについて、30 の固有の登録組織と 21 の ISP を確認しました。この手法により、セキュリティ研究者がドメインを関連付け、アクターのインフラストラクチャを区別することがより困難になります。

`b36cname` レコードを持つドメインの登録メタデータのバリエーションから、当初私たちはこのアクターが詐欺キャンペーンを実行している他のサイバー犯罪者のサービスプロバイダーである可能性があると疑いました。しかし、私たちの分析により、彼らのネットワークを介して実行される金融詐欺キャンペーンはすべて同じ要素と全体的な動作を共有していることが判明し、キャンペーンはおそらく単一のアクター、Savvy Seahorse によって制御されているという結論に至りました。これらのキャンペーンとその内容については、キャンペーン分析のセクションで詳しく説明します。

IPアドレス

Savvy Seahorse は約 50 個の専用 IP アドレスを使用し、図 5 に示すように定期的に変更しているようです。各タイムラインバーの小さなギャップは、Savvy Seahorse が CNAME レコードに関連付けられた IP を変更した時期を表しています。

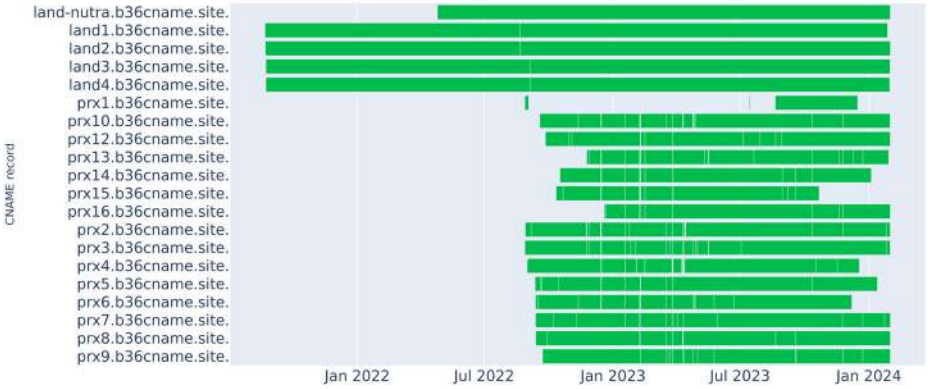


図 5：*CNAME* による *IP* アドレス変更のタイムライン。各バーは各 *CNAME* レコードが特定の *IP* アドレスに費やした時間を示し、狭い隙間はこれらの値がいつ変更されたかを示します。攻撃者は検出を回避するために *IP* アドレスを頻繁に変更しています。

IP の変更の分析に基づいて、次のことがわかりました。

- `land-nutra[.]b36cname[.]site` は 1 つの IP アドレスを持つ唯一の CNAME であり、この CNAME に関連付けられた空ドメインであることを示す動作と一致しています。この IP アドレスには、全体的に非常に多くのドメインが関連付けられていて、この特性は空ドメインの IP アドレスと一致しています。

8 https://blogs.infoblox.com/cyber-threat-intelligence/rdgas-the-new-face-of-dgas/

- land<1-4>[.]b36cname[.]site パターンを使用する 4 つの CNAME はすべて、IP アドレスが 1 回だけ変更されています。
- prx<1-16>[.]b36cname[.]site の CNAME は IP アドレスを頻繁に変更しています。このパターンは、IP の定期的な変更が脅威アクターがセキュリティベンダーによる検出とブロックを回避するために使用する戦術であるため、これらの IP がアクティブな詐欺キャンペーンにのみ使用される可能性が最も高いことを示しています。
- 脅威アクターが複数の CNAME の IP を同じ値に同時に変更するケースがいくつかあります。
- prx6[.]b36cname[.]site や prx15[.]b36cname[.]site などのいくつかの CNAME は、現在脅威アクターによって使用されていないようです。

キャンペーン分析

Savvy Seahorse は独自のインフラストラクチャを使用して、金融や投資をテーマにしたさまざまな詐欺キャンペーンを実行しています。これらのキャンペーンは、様々な高度な誘い出しテクニックを特徴としていますが、金銭的な利益を得るために被害者の個人情報や金銭的な情報を盗むことを最終目的として、どれも似たようなパターンをたどります。これらのキャンペーンで使用される言語には、英語、ロシア語、ポーランド語、イタリア語、ドイツ語、フランス語、スペイン語、チェコ語、トルコ語が含まれます。

- アクティブなキャンペーンはサブドメインレベルで運営され、各サブドメインには prx<1-16>[.]b36cname[.]site の CNAME レコードがあります。

キャンペーンの詳細

Savvy Seahorse は、各 Web ページに埋め込まれた登録フォームを使用して、被害者の氏名、メールアドレス、電話番号を収集します。この登録フォームの 2 つの例（1 つはポーランド語、もう 1 つは英語）を図 6 に示しています。

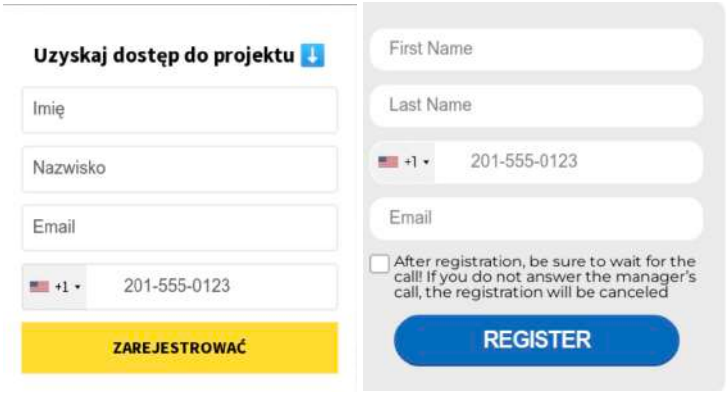


図 6：Savvy Seahorse のキャンペーンで使用された登録フォーム

検証とリダイレクト

ユーザーがこれらのフォームに情報を入力すると、ドメインは Savvy Seahorse がキャンペーンで使用するセカンダリ TDS ドメイン getyourapi[.]site にアクセスし、ユーザーの IP アドレス、位置情報、提供された電話番号とメールの有効性など、情報の検証チェックを実行します。どのチェックに合格するかによって、次の 3 つの異なるシナリオが観察されています。

1. フォームデータは有効でも、ユーザーが以前に同じメールアドレスや電話番号を使用して登録した場合、Web ページにはユーザーがすでに登録済みと表示されます。
2. フォームデータは有効でも、ユーザーが以前に同じ IP アドレスでこのドメインにアクセスしたことがある場合、ページには登録を確認するメッセージと、担当者が追加情報を求めて電話することを伝えるメッセージが表示されます。リダイレクトは行われません。
3. フォームデータが有効で、ユーザーがなじみのないIPアドレスでドメインにアクセスすると、図7のような偽の取引ウェブページにリダイレクトされます。

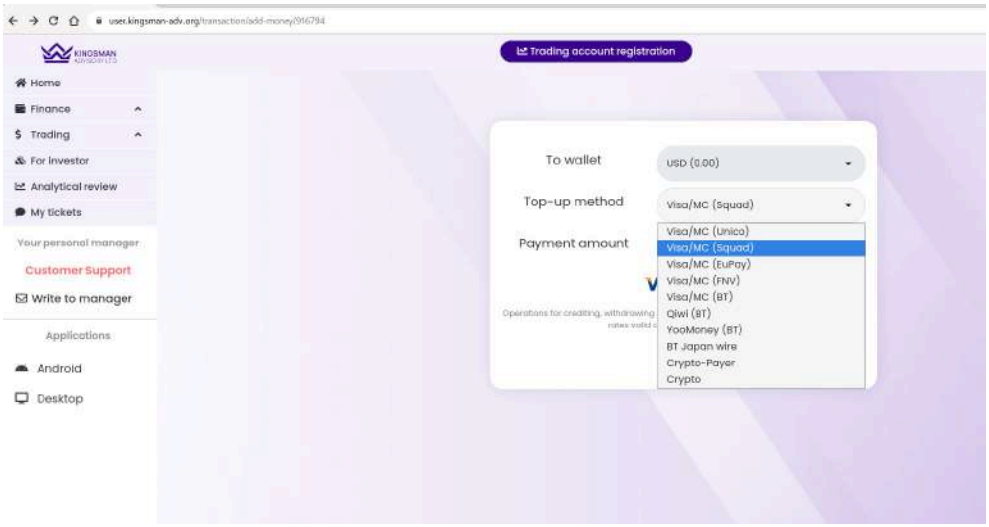


図 7：*Savvy Seahorse* の偽の取引プラットフォーム

注目すべき重要な詳細として、攻撃者はユーザーの情報を検証して、ウクライナ、インド、フィジー、トンガ、ザンビア、アフガニスタン、モルドバなど、事前に定義された国のリストからトラフィックを除外していることが挙げられますが、これらの特定の国を選択した理由は不明です。最初の検証チェックは、登録フォームに入力された電話番号に対して行われます。電話番号がブロックリストに載っている国のいずれかからのものだった場合、Web ページには「**このプログラムはお住まいの地域ではサポートされていません**」というメッセージが表示されます。ユーザーが前述のように、受け入れ可能な電話番号とその他の有効な情報をすべて入力すると、攻撃者はその情報をセカンダリ TDS ドメインに送信して、除外された国に対してユーザーの IP アドレスの地理的位置を検証し、リダイレクトするかどうかを決定します。

取引プラットフォーム

ユーザーがリダイレクトされると、偽の取引プラットフォームは登録フォームに入力された詳細を使用して自動的にアカウントを設定します。このプラットフォームは非常に洗練されているようで、デスクトップアプリケーションをダウンロードするオプションと、App4World と呼ばれる Google Play ストアの Android アプリへのリンクを提供しています。

その後、ユーザーは、Visa/Mastercard、暗号通貨ウォレット、Qiwi や YooMoney などのロシアの決済プロバイダーなど、さまざまなソースから自分の「ウォレット」に資金を追加するよう促されます。ウォレットにお金を追加するには、最低 50 米ドルの「トップアップ（補充）」金額が必要になります。ユーザーが支払い元と入金額を指定すると、8 つの支払い処理ドメイン（表 5 を参照）のいずれかに最終的にリダイレクトされます。キャンペーンが被害者から財務情報を収集するためにどのドメインを使用するかは、被害者がどのソースから送金するかによって異なります。

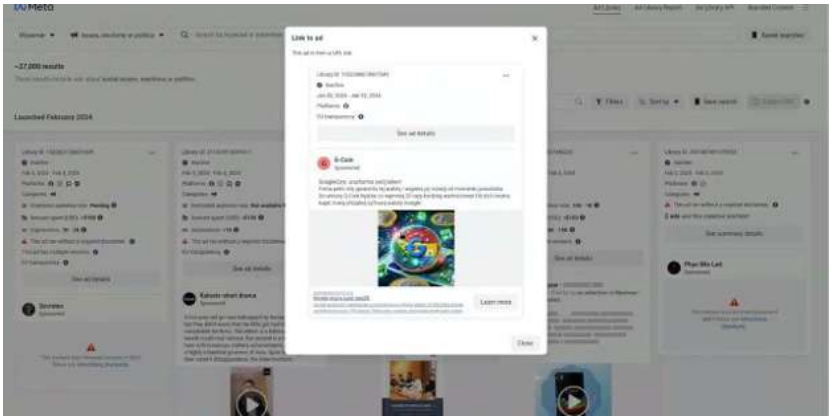
支払い元	支払ドメイン	支払いドメインの説明
Visa/MC (Unico)	makeyourpay[.]com	支払い処理 Web ページをホストする新規登録ドメイン、ロシア語のサブドメイン
Visa/MC (Squad)	checkout[.]flutterwave[.]com	ナイジェリアに拠点を置く合法的な金融インフラ会社をホスト
Visa/MC (EuPay)	ap-gateway[.]mastercard[.]com	Mastercardの正規の支払いゲートウェイ
Visa/MC (BT)	sci[.]pointpayment[.]net	他の多くの疑わしい決済ドメインと同じ専用 IP でホストされている
Qiwi (BT)	qiwi[.]bppsa[.]com	ベースドメインはロシア語の支払い処理 Web ページをホスト
YooMoney (BT)	ymoney[.]bppsa[.]com	ベースドメインはロシア語の支払い処理 Web ページをホスト
BT Japan (電信)	processing[.]betatransfer[.]io	高リスク決済処理サービスである Betatransfer Kassa の API (主にオンラインギャンブルに使用されている)
Crypto-Payer Crypto	crypto-payer[.]co	2023 年 12 月登録

表 5：被害者の財務情報を収集するための支払い処理ドメイン

調査の結果、図 8 に示すように、攻撃者は少なくとも 1 つの支払い処理ドメイン (sci[.]pointpayment[.]net) について、ロシア国有銀行の SberBank に資金を送金していることが判明しました。

図 8：sci[.]pointpayment[.]net の財務詳細

以下の動画では、偽の取引プラットフォームを手順を追って説明しています。



Savvy Seahorse Campaign Walkthrough をご覧ください。

Meta ピクセル

Savvy Seahorse はこれらのキャンペーンを Facebook/Meta 広告経由で販売し配信しているため（図 9 を参照）、アクティブなキャンペーンで使用されるすべてのドメインは connect[.]facebook[.]net と www[.]facebook[.]com に複数の接続を確立します。攻撃者はまた、本物のツールである Meta ピクセルを使用して、広告のパフォーマンスを追跡して最適化します。[9]

Meta ピクセルは、次の 2 つの部分で構成される JavaScript コードです。

- ページが読み込まれ、Facebook ピクセルが初期化され、「PageView」イベントを追跡するときに実行される「script」。
- ユーザーがブラウザで JavaScript を無効にしている場合に実行される「noscript」。このセクションでは、イベントを追跡するための 1x1 ピクセル画像が表示されます。

各 Meta ピクセルには、Facebook への HTTP 接続で確認できる一意の ID 番号が付いています。同じ SLD でホストされ、異なるサブドメインが同じ ID を共有しているキャンペーンもありますが、他のキャンペーンはランダム化されているようです。

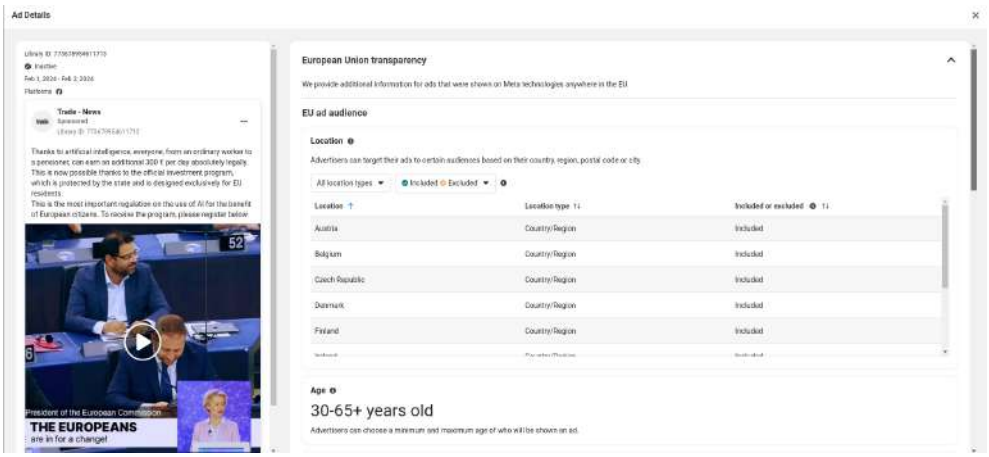


図 9：ターゲット国と年齢層を表示している *Savvy Seahorse* のキャンペーンの *Facebook* 広告の詳細

9 https://www.facebook.com/business/tools/meta-pixel

テーマ

Savvy Seahorse のキャンペーンの具体的なテーマは多岐にわたり、投資機会を求めて Apple などの正当な企業になりすましたり、WhatsApp、ChatGPT、Tesla になりすますボットを組み込んだりするものもあります。

企業を装った収益プロジェクト

Savvy Seahorse が運営を通じて最も頻繁に使用してきたテーマの 1 つは、ユーザーが個人情報を登録すれば特定の金額を稼ぐチャンスがあると主張する「収益プロジェクト」または投資プログラムです。脅威アクターは、ユーザーとの信頼関係を築くために、わかりやすいブランドや企業になりすまそうとする一般的なフィッシングキャンペーン手法を採用することがよくあります。表 6 は、これまでに確認したいくつかの例を示しています。

キャンペーンサブドメイン	関連する CNAME	キャンペーン内容
new[.]xsdelx[.]top	prx2[.]b36cname[.]site	Tesla と X に偽装し、ユーザーに「Elon Musk のプロジェクトに参加」して毎月 1 万 2000 ユーロを受け取るよう勧めているロシア語のキャンペーン
bwn[.]objectop[.]xyz	prx7[.]b36cname[.]site	正当なカナダの石油会社である Imperial Oil を装った英語のキャンペーン。インタラクティブな「アンケート」があり、ユーザーに 250 ドルから 1,000 ドルの投資を促すランディングページ
sej[.]progmedisd[.]site	prx9[.]b36cname[.]site	Mark Zuckerberg が考案したと主張し、ユーザーに最大 30 万ポーランドズウォティ（PLN）の収益を約束する「Libra 自動収益プロジェクト」の 2023 年 2 月からのポーランド語のキャンペーン

表 6：*Savvy Seahorse* の金融関連キャンペーンの例

図 10 と 11 は、表 6 のキャンペーンの一部のスクリーンショットを示しています。Savvy Seahorse がなりすました他の企業の例としては、Apple、Meta、Mastercard、Visa、Google などがあります。

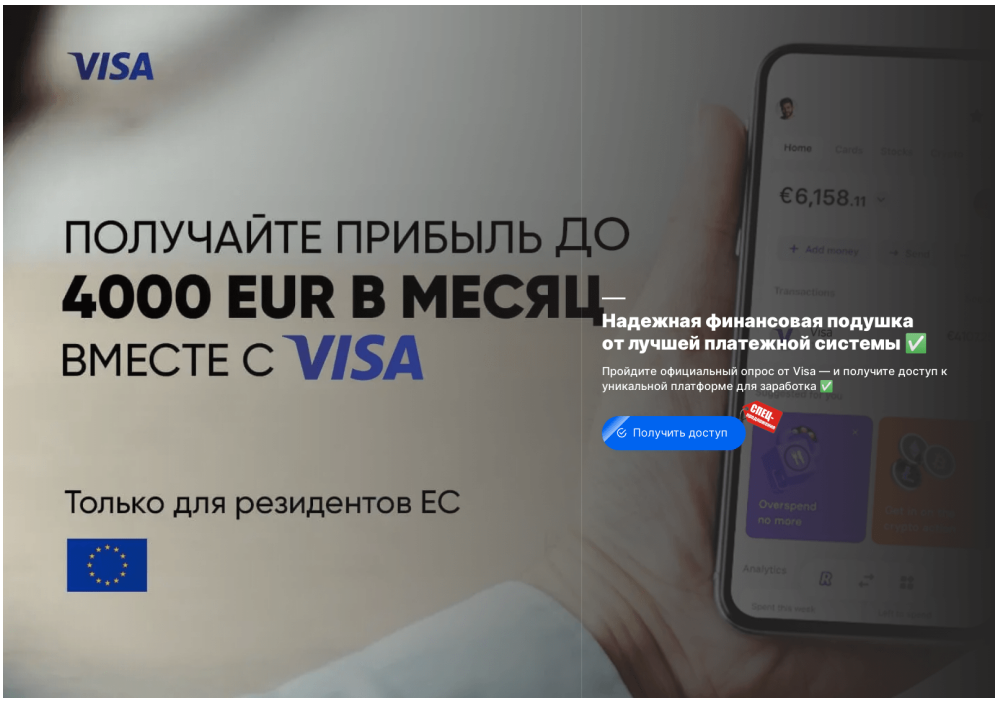


図 *10*：*Visa* を偽装したロシア語キャンペーンの visa[.]lukzev[.]xyz のランディングページ

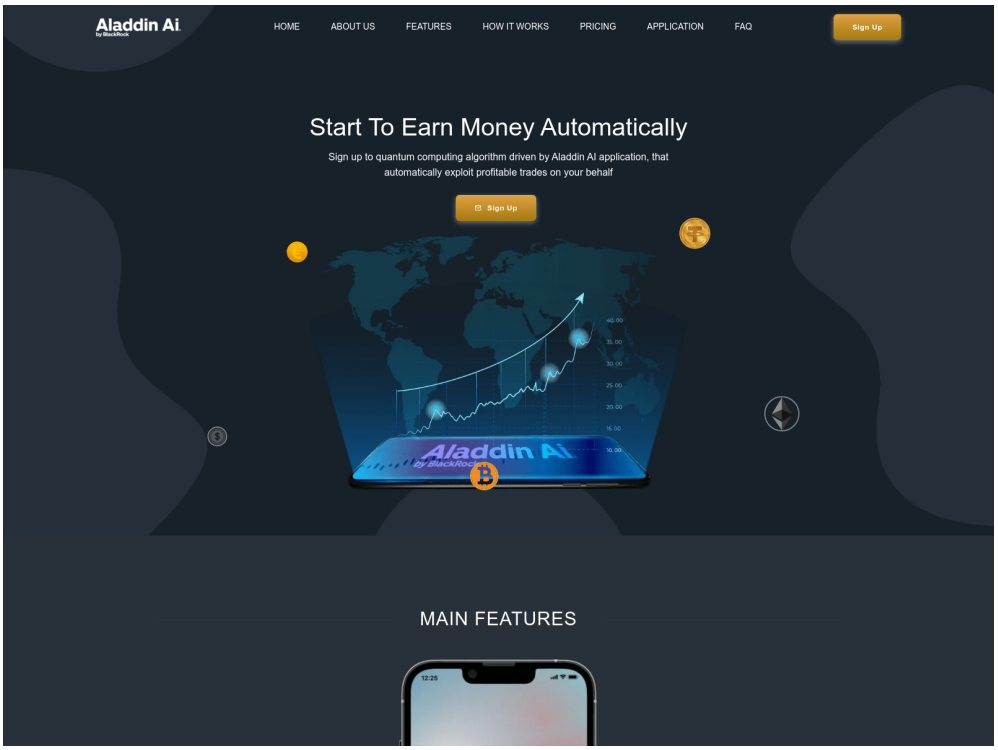


図 *11*：*BlackRock* のポートフォリオ管理プラットフォームを偽装した adin[.]czproftes[.]xyz のランディングページ

偽ボット

ChatGPT、WhatsApp、Tesla などを装ったチャットボットを使った高度な誘導手法を特徴とするキャンペーンがいくつか確認されています。最近、この種のボットを使った詐欺は、ユーザーの信頼を得て個人情報を盗もうとする脅威アクターの間で一般的な傾向になっています。[10]図 12 のスクリーンショットは、Tesla になりすましたキャンペーンのチャットボットとのやり取りを示しています。

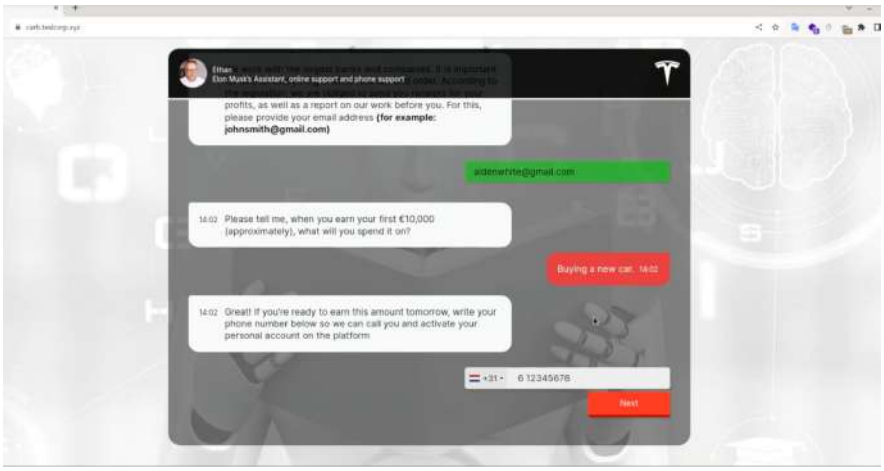


図 *12*：*Savvy Seahorse* キャンペーンで使用された偽の *Tesla* をテーマにしたボット

ボットは、潜在的な収益と投資の機会への関心についてユーザーに質問しますが、最終的には他のキャンペーンと同じパターンに従います。つまり、偽の取引プラットフォームにリダイレクトする前に、ユーザーに個人情報の登録を促します。

結論

Infoblox では、脅威の攻撃者が DNS を悪用して犯罪行為を隠蔽する新たな方法を見つけることに引き続き注力しています。Savvy Seahorse が DNS CNAME を TDS として使用して悪意のある操作を管理する手法は、DNS がサイバー犯罪者の活動を追跡して阻止する最も効果的な方法であることを示しています。CNAME パターンの分析により、最終的にこの行為者と、大規模な詐欺キャンペーンのネットワークを運用するために使用している独自の戦術、技術、手順 (TTP) を発見することができました。

10https://www.security.org/digital-security/guide-to-chatbot-scams/

活動の指標

以下は、Savvy Seahorse のキャンペーンで使用されている指標のサンプルです。より包括的な指標のリストはこちらの GitHub リポジトリにあります。

指標	指標の種類
getyourapi[.]site	Savvy Seahorse セカンダリ TDS ドメイン
land-nutra[.]b36cname[.]site	パークドメインの CNAME レコードとして使用されたサブドメイン
land<1-4>[.]b36cname[.]site	非アクティブなキャンペーンの CNAME レコードとして使用されたサブドメイン
prx<1-16>[.]b36cname[.]site	アクティブなキャンペーンの CNAME レコードとして使用されたサブドメイン
new[.]xsdelx[.]top bwn[.]objectop[.]xyz sej[.]progmedisd[.]site adin[.]czproftes[.]xyz visa[.]lukzev[.]xyz sun[.]autotrdes[.]top hmz[.]coivalop[.]xyz news[.]beneffit[.]top goiin[.]baltez-offic[.]xyz	アクティブな Savvy Seahorse キャンペーンのサブドメイン
ultra-vest[.]one kingsman-adv[.]org abyss-world-asset[.]net	一部のキャンペーンでユーザーがリダイレクトされる偽の取引ウェブサイト
sci[.]pointpayment[.]net makeyourpay[.]com qiwi[.]bppsa[.]com ymoney[.]bppsa[.]com processing[.]betatransfer[.]io crypto-payer[.]co	被害者の財務情報を収集するための支払い処理ドメイン

指標	指標の種類
ap-gateway[.]mastercard[.]com	被害者の財務情報を収集するために使用された Mastercard の正規ドメイン
checkout[.]flutterwave[.]com	被害者の財務情報を収集するために使用されたナイジェリアの決済サービス、Flutterwave の正規ドメイン
auproject[.]xyz badanie-pl[.]site blog-vcnews[.]site capital-inwest[.]site dasms[.]xyz duums[.]xyz esbopehan[.]xyz	Savvy Seahorse ベースドメイン

INFOBLOX THREAT INTEL

Infoblox Threat Intel は、独自の DNS 脅威インテリジェンスを作成している大手企業であり、数多くの情報収集サイトの中でも際立っています。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。私たちは防御するだけでなく、先を見越して、私たちのインサイト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支援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 Detection and Response 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.

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

© 2024 Infoblox, Inc.All rights reserved.Infoblox ロゴ、およびここに表示されているその他のマークは、Infoblox, Inc. の所有物です。
他のすべてのマークは、それぞれの所有者に帰属します。

バージョン: 20240216v1