infoblox

Threat Intel

PROLIFIC PUMA:
サイバー犯罪を可能にする偽装リンク短縮サービス

著者
ローラ・ダ・ロシャ
レニー・バートン
ステリオス・チャツィストギアス
ダービー・ワイズ

目次

全体の概要

ハロウィーンは一年で最も不気味な時期かもしれませんが、脅威アクターは毎日インターネット上で恐ろしいことをしています。先月、私たちは Domain Name System（DNS）の脅威アクターと RDGA（登録ドメイン生成アルゴリズム）という 2 つの用語を紹介しました。また、Open Tangle の暴露を通じて、DNS 脅威アクターの 1 つのタイプである執拗なフィッシング詐欺師について少し触れました。

本書では、このシリーズ 2 番目のアクターである **Prolific Puma** を紹介します。4 年、あるいはそれ以上の間、Prolific Puma は防御側に気づかれずに活動していました。その起源は把握されていませんが、私たちは DNS を通じて Prolific Puma を検出し、ドメイン名登録の選択からその特徴を垣間見ることができます。名前の由来は何でしょうか。「Prolific（多く生成される、多産の）」は、このネットワークが継続的に拡大しており、ほぼ毎日新しいドメインが登録されているという単純な事実に由来しています。「Puma」については、この資料の後半でその着想について詳しく説明します。

サイバー犯罪経済は世界で 3 番目の規模を持ち、2023 年には 8 兆ドルの価値に達したと推定されており、Prolific Puma はそのサプライチェーンの一部です。[1]Prolific Puma は RDGA を使用してドメイン名を作成し、これらのドメインを使用して他の悪意のあるアクターに URL 短縮サービスを提供し、そのアクターがフィッシング、スパムメール、およびマルウェアを配布する間の検出回避を助けています。Prolific Puma を破壊すれば、犯罪経済のより大きな部分を破壊できることになります。図 1 は、Prolific Puma の活動の概要と、それが犯罪者にとって役立つ仕組みを示しています。Prolific Puma はアルゴリズムによって大量のドメインを生成し、それらのドメインを使用して、他の悪意のあるアクターのための短縮 URL を生成し、実際の活動を隠蔽します。

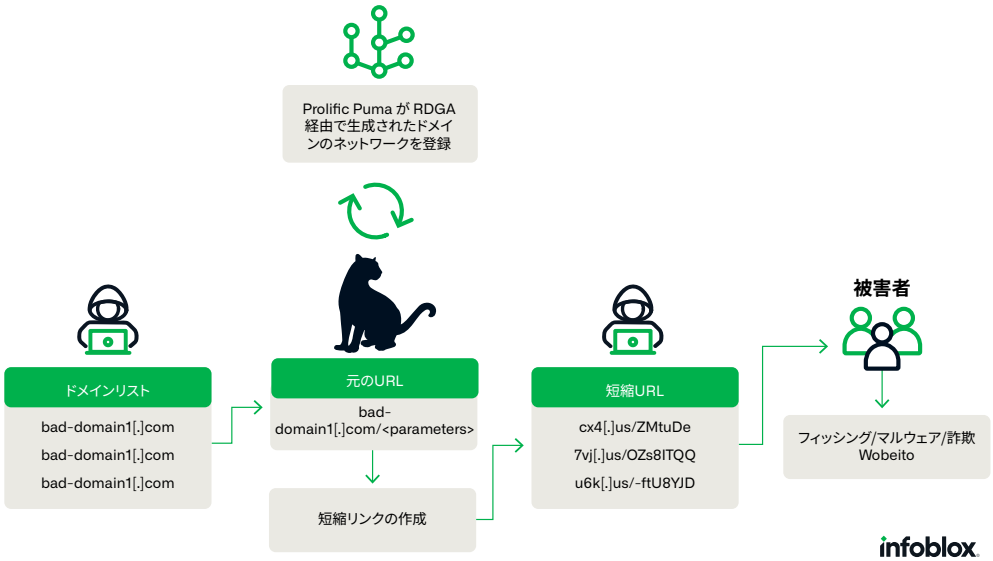


図 *1.* サイバー犯罪サプライチェーンにおける *Prolific Puma* の役割の概要。

私たちの知る限り、本資料は大規模な地下 URL 短縮サービスに関する最初の記述です。さらに、**このアクターはマルウェアやフィッシングサイトからではなく、DNS 分析から発見されました。**Prolific Puma が注目されるのは、18 か月以上にわたって悪意のあるアクティビティを円滑化しても、セキュリティ業界で気付かれずにいたことです。膨大なドメイン名のコレクションを利用して、悪意のあるトラフィックを配信し、検出を回避できます。

1 https://cybernews.com/editorial/cybercrime-world-third-economy/

この発見は、DNS とドメイン登録データを使用することで、疑わしいアクティビティを検出するだけでなく、その情報をまとめて DNS 脅威アクターの統合ビューを作成することも可能であることを示しています。私たちは、DNS を介して Prolific Puma を検出し追跡することができましたが、一般的な実例を見ると、ドメインレジストラとレジストリが不正使用を制御するために直面している課題が浮き彫りにされています。アクターが実際の犯罪から遠ざかっていると、犯罪を可能にするドメインの特定と削除をポリシーが妨げる場合があります。

6 か月前私たちは**、RDGA 検出機能によって初めて Prolific Puma のドメインを認識しました。**それ以来、私たちは Prolific Puma のネットワークの拡大を追跡する専用の DNS 検出機能を使用して、そのアクティビティに対する理解を深めてきました。次のセクションでは、Prolific Puma URL 短縮サービス、ドメインの登録とホスティングの方法、米国トップレベルドメイン（usTLD）の悪用、インターネット犯罪の促進における役割について説明します。本資料では、そのサービスを使用するキャンペーンではなく、アクターと DNS の使用に意図して焦点を当てています。ここでは、Prolific Puma のインフラストラクチャを使用して実行されたキャンペーンの詳細な例を 1 つご紹介します。このキャンペーンは、ユーザーへのフィッシングとブラウザベースのマルウェアの配信の両方につながりました。

偽装 URL 短縮サービス

Prolific Puma は犯罪者に偽装 URL 短縮サービスを提供しています。[2] アクティブな第 2 レベルドメイン（SLD）に直接アクセスすると、次のメッセージが返されます。

```
{“type”: “service”,”name”:”@link-shortener/handler-service”}
```

URL 短縮サービスの本来の目的は、ウェブサイトのリンクを簡単に共有できるようにすることと、ソーシャルメディアのサイズ制限に収めることでした。例えば、

- リンク `https://tinyurl.com/c6u6myhw` は、
- https://blogs.infoblox.com/cyber-threat-intelligence/introducing-dns-threat-actors/ の短縮バージョンで、この URL は DNS 脅威アクターの概念を紹介した論文です。

ユーザーが短縮リンクをクリックすると、別の URL にリダイレクトされます。内部的には、短縮サービスドメイン（例：`tinyurl[.]com`）の IP アドレスを解決するための DNS 要求が行われます。その後、元のサイトを識別するために使用されるハッシュ値を含む Web 要求がそのアドレスに送信されます。上記の例では、TinyURL サービスは値 c6u6myhw を使用して、接続をリダイレクトする場所を決定します。最終的なコンテンツをホストする IP アドレスを見つけるために、追加の DNS 要求が行われます（この場合は `blogs.infoblox.com`）。正当なユーザーは共有するために単純な短縮リンクを作成しますが、悪意のある攻撃者は最終的なランディングページの前に複数のリダイレクトレイヤーを使用する場合があります。このプロセスは図 2 に示されています。

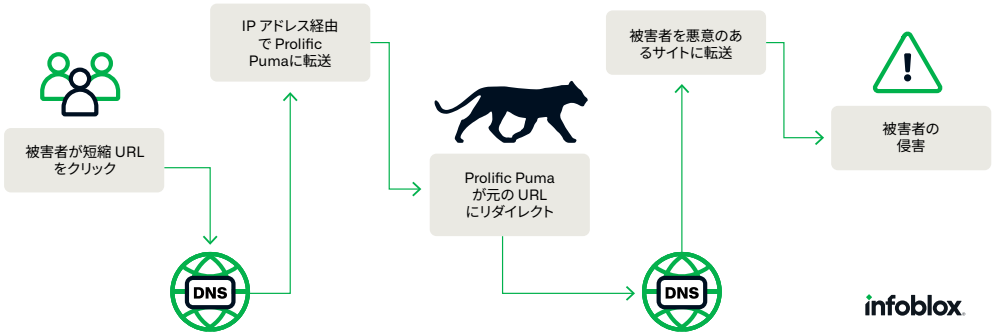


図 2：短縮 *URL* が *DNS* および短縮サービスと連携して、被害者を悪意のあるコンテンツにリダイレクトする仕組みを示す概念図。

2 https://en.wikipedia.org/wiki/URL_shortening

悪意のあるアクターがリンク短縮サービスをフィッシングに悪用することが知られています。[3] しかし、最もよく知られている事例では、リンク短縮サービスは、TinyURL、BitLy、Google などのよく知られた公開サービスです。この悪用は非常に蔓延しているため、マーケティング会社の Rebrandly は、合法的な企業にはメールで人気の短縮ツールを使用しないことを推奨しています。[4]

Prolific Puma は自社のサービスを公に宣伝していません。しばらくの間、当社はリンク短縮サービスを追跡していることはわかっていましたが、そのサービスが提供している内容や、誰にサービスを提供しているのかは不明でした。リンク短縮サービスの調査で難しいのは、完全な URL がないと、最終的なランディングページを特定できないということです。私たちの検出機能は、疑わしい振る舞いをしていて公開されていない、相互接続されたドメインを大量に発見しましたが、それらがどのように利用されているかを結論付けるのは困難でした。

結果的に、フィッシングサイトや詐欺サイトであるランディングページに、最終的にはリダイレクトする短縮リンクの事例を数件確認しました。興味深いことに、最終ページへのリダイレクトの順序は大きく異なっていました。場合によっては、短縮リンクが直接コンテンツにつながっていることもあります。[5] 他のサイトでは、最終的なランディングページに到達する前に、複数のリダイレクトレイヤーが発生しました。[6] また、Prolific Puma の短縮リンクが別のサービスによって作成された別の短縮リンクにリダイレクトされることも確認されました。[7] 場合によっては、短縮リンクから CAPTCHA チャレンジが表示されることがあります。[8] また、2020 年 1 月には、偽の Amazon 配送通知の SMS テキストメッセージ経由で Prolific Puma リンクが送信されていたという報告も見つかりました。[9] リンクの扱い方やコンテンツの配信方法にばらつきがあることから、Prolific Puma が複数の主体にサービスを提供している可能性が高くなります。エビデンスによると、短縮リンクは主にテキストメッセージを通じて被害者に配信されますが、ソーシャルメディアや広告など、他の文脈でも使用される可能性があります。

Prolific Puma は、私たちが発見した唯一の違法リンク短縮サービスではありませんが、最大規模で最も動的なサービスです。この短縮サービスを通じて配信される合法的なコンテンツは見つかりませんでした。このレポートの後半では、ユーザー情報のフィッシング、詐欺的な支払い、ブラウザマルウェアの配信につながる短縮リンクの具体的な例について詳しく説明します。

サイバー犯罪エコシステム内のサービスプロバイダーとして、Prolific Puma は、他の悪意あるアクターによる検出回避を手助けしており、検出回避はエンタープライズ MITRE ATT&CK フレームワークに含まれる戦術です。[10] しかし、フィッシング、詐欺、マルウェアを消費者に届ける際の間接的な役割も、検出回避を手助けします。セキュリティプロバイダーは最終的なコンテンツを特定し、ブロックすることはできますが、より広い視野を持たなければ、アクティビティの全容を把握し、ドメインを単一の DNS 脅威アクターの下に関連付けることは困難です。次に見るように、私たちは DNS 分析を通じてこれを行うことができます。

3 https://portswigger.net/daily-swig/cybercriminals-use-reverse-tunneling-and-url-shorteners-to-launch-virtually-undetectable-phishing-campaigns

4 https://support.rebrandly.com/hc/en-us/articles/228632488-Blacklisted-URL-Shorteners-Stop-Using-Them-in-Emails-

5 https://urlscan.io/result/3be86d9f-e596-4a9b-9260-d331811262e5/

6 https://urlscan.io/result/00c1d82d-0f03-44b6-96d3-63b503fff464/

7 https://urlscan.io/result/26077ac3-1559-4329-ab48-120181555586/

8 https://urlscan.io/result/726b6baa-d259-4f67-a4f9-aef3bd93aca3/

9 https://turbolab.it/amazon-2444/sms-amazon-hai-messaggio-riguardante-articolo-nome-arrivato-3.-classifica-2960

10 https://attack.mitre.org/tactics/TA0005/

検出とドメイン名の特徴

クラウドおよびオンプレミスの Infoblox DNS Detection and Response 製品に独自のインテリジェンスを提供するために、当社は疑わしいドメインや悪意のあるドメイン、関連する IP アドレス、およびその他の DNS リソースを検出するための独立したアルゴリズムの大規模なコーパスを設計しました。**パッシブ DNS（pDNS）クエリログおよびその他のデータソースを集約することにより、新たにクエリ、登録、または構成されたドメインのコレクションに対して一連の分析を実行します。**これらの分析はドメインを個別に特徴付け、ドメインを疑わしいものとしてフラグ付けすることから、DNS 脅威アクターに割り当てることまで多岐にわたります。

Prolific Puma の発見は、私たちが社内で命名し追跡している多くの DNS 脅威アクターに共通する経路へと繋がりました。当社の自動化された分析により、最初にいくつかの関連ドメインが個別に疑わしいとラベル付けされました。この判定により、ドメインを DNS 再帰リゾルバーでブロックして顧客を保護することができましたが、必ずしもアクティビティの全容を捉えたわけではなく、複数ドメインを単一のアクターに関連付けることもしませんでした。**2023 年春に RDGA 検出のアルゴリズムを導入したとき、Prolific Puma ドメインが複数のグループで識別され始めました。**これらのグループも自動的に決定されましたが、RDGA ドメインが同じ DNS 脅威アクターによって登録されたという高い信頼性を確保するために統計的手法が使用されました。最後に、別のアルゴリズムが IP 解決の異常な動作を識別し、個々の RDGA クラスターを関連付けました。アクティビティの規模の大きさから、この特定の DNS 脅威アクターはヒューマンインザループ調査の対象となり、追跡専用の DNS フィンガープリントを設計しました。このセクションの残りの部分では、Prolific Puma ドメイン名の特徴と、それらを識別する機能について詳しく説明します。

Prolific Puma のドメインと最終的なランディングページとの間の接続は間接的であるため、アクターは検出からある程度保護されています。しかし、彼らはまた、大量のドメインの登録を通じて、長期間気づかれない状態を保つ能力を強化します。悪意のあるトラフィックは、これらのドメイン間でかなり細かく分かれます。時間が経つにつれて、ドメインは戦略的エイジングの結果として「優良」として評価されることさえあります。Prolific Puma が使用したこの手法については、本資料の後半で詳しく説明します。

Prolific Puma は、私たちが追跡している最大級のネットワークを管理しています。2022 年 4 月以降、彼らは 35,000 から 75,000 の独自ドメイン名を登録しています。図 3 は、3 つまたは 4 つの長いドメインラベルを使用して、1 日に登録された独自ドメイン名の数を示しています。最近報告したように、RDGA は従来の DGA に取って代わりつつあり、防御者にとって新たな課題の種となっています。この手法を使うことで、彼らはその手口を容易に自動化し、拡大できます。Prolific Puma ドメインは、Infoblox が毎日検出する、RDGA によって生成された何千もの新しいドメインに含まれています。

Prolific Puma はドメイン名レジストラとして NameSilo を使用しており、匿名プロバイダーでサービスをホストする前にドメインを戦略的に古くする傾向があります。米国との明確な関係がないにもかかわらず、Prolific Puma は米国市民および組織のために予約されている TLD である米国トップレベルドメイン（usTLD）を継続的に悪用しています。Prolific Puma は、新しいドメインと削除されたドメインの両方を登録することで知られています。たとえば、3ty[.]us は、2022 年 6 月に別の攻撃者によって Facebook メッセンジャーのフィッシングキャンペーンに使用され、2023 年 7 月に登録が失効した後、Prolific Puma によって登録されました。

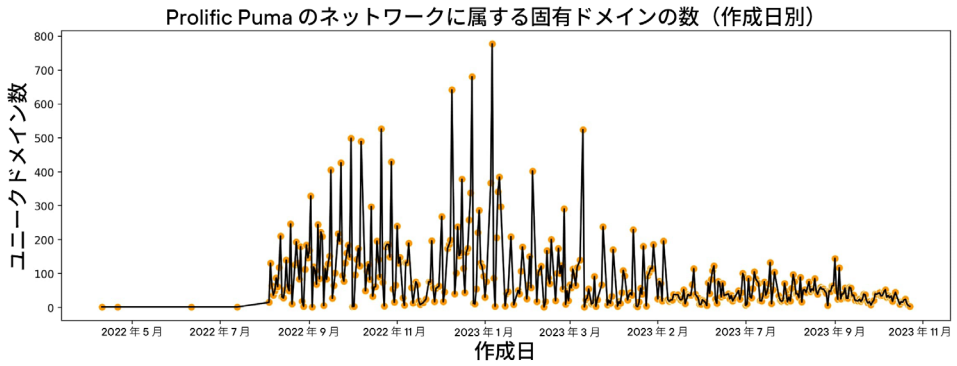


図 *3. 3 ～ 4* 文字のドメインラベルを含む *Prolific Puma* ドメインの登録を表すタイムライン。

Prolific Puma ドメインは英数字で、疑似ランダム、長さは可変で、通常は 3 文字または 4 文字ですが、7 文字の SLD ラベルも確認されています。ドメインは、悪意のある攻撃者に頻繁に悪用される 13 の TLD に登録されており、その中には `info`、`us`、`site`、`in`、`link`、`me`、`cc`、`website`、`life`、`xyz`、`club`、`buzz`、および `best` が含まれます。2023 年 5 月までは、infoTLD がドメインの大部分を占めていました。それ以降、攻撃者は作成したドメイン全体の約 55% に usTLD を使用しています。2023 年 5 月以降、平均して 1 日あたり 43 の新しいドメインが確認されています。

TLD	us	link	info	com	cc	me
ドメイン	vf8[.]us	cewm[.]link	uelr[.]info	kfwpr[.]com	jlza[.]cc	scob[.]me
	2ug[.]us	wrzt[.]link	ldka[.]info	trqrh[.]com	hpko[.]cc	xnxk[.]me
	z3w[.]us	hhqm[.]link	fbvn[.]info	nhcux[.]com	ddkn[.]cc	zoru[.]me
	yw9[.]us	ezqz[.]link	baew[.]info	khrig[.]com	mpsi[.]cc	mjzo[.]me
	8tm[.]us	zyke[.]link	shpw[.]info	dvcgg[.]com	wkby[.]cc	ouzp[.]me

表 1：3 ～ 4 文字のドメインラベルを含む、さまざまな TLD で Prolific Puma によって登録されたドメインの例。

***Infoblox* は、分析機能として幅広い評価スコアを使用しています。当社の評価アルゴリズムは公開されており、すべてのデータタイプに適用され、統計的に最適であるため、同じデータを使用する別のアルゴリズムの方が正確ということはありません。スコアは、時間とデータタイプにわたって一貫して解釈できる正規分布に調整されます。スコア *7* は高リスクと見なされ、平均より *1.5* ～ *3.5* ほど標準偏差が上です。レジストラの評価とネームサーバーの評価の履歴分析は、それぞれ *2022* 年第 *3* 四半期と第 *4* 四半期の四半期脅威インテリジェンスレポートに記載されています。**

過去 18 ヶ月間、Prolific Puma は主に NameSilo を登録とネームサーバーに使用していました。安価なドメイン名とホスティングのプロバイダーである NameSilo は、悪意のあるアクターによって頻繁に悪用されています。手頃な価格もさることながら、多くのレジストラと同様に API を提供しているため、合法的なユーザーと犯罪者の両方にとって一括登録がしやすくなっています。NameSilo でドメインを登録する際に必要なのは、メールアドレスと支払い方法だけです。しかし、ドメインを使用するための設定には、名前と物理的な住所が必要です。登録されているものの未設定のドメインは保留されます。DNS を通じて返される IP アドレスは SEDO Gmbh に属し、レジストラに提供されるプレミアム SEDO マルチリスティングサービスの一部です。

Infoblox の評価アルゴリズムによると、NameSilo は悪用されやすいレジストラです。現在、NameSilo に登録されたドメインのリスクは 0 から 10 の尺度で 7 と評価されています。10 は極めて高いリスク、5 は平均的なリスクとみなされています。TLD に加えて、ネームサーバーにも評価アルゴリズムを適用できます。Prolific Puma は、dnsowl[.]com ドメイン内にある NameSilo のデフォルトのネームサーバーを使用します。[11] 当社のアルゴリズムは現在、dnsowl[.]com ネームサーバーのリスクを 6 と評価しています。これは中程度ですが、他のすべての既知のネームサーバーと比較するとわずかに高いリスクです。

DNS の脅威アクターがオペレーションに単一のレジストラを使用することは珍しいことではありませんが、頻繁に起こることでもありません。そのため、単一レジストラの使用は、DNS 脅威アクターに関する当社の分類では、特徴とされています。私たちが追跡しているアクターは、概して 1 年以上継続しており、多くの場合、金銭的な動機があります。多くの場合、最も安価で手間がかからないレジストラと TLD が選択されていることが判明しています。NameSilo は安いレジストラですが、唯一のレジストラではありませんし、長期にわたってドメインの最安値を提供するわけではありません。過去に、Prolific Puma は他の安価なプロバイダー、特に NameCheap に多数のドメインを登録しました。NameSilo が長期間にわたって一貫して使用されていることは注目に値しますが、その動機は不明です。

USTLD の悪用

Prolific Puma は、2023 年 5 月以降、usTLD に何千ものドメインを登録しています。usTLD Nexus Requirements Policy によれば、米国市民または米国関連の企業のみが usTLD にドメインを登録できるため、これは注目に値します。[12] さらに、usTLD では透明性が求められており、ドメイン名を非公開で登録することはできません。その結果、ドメインに関連付けられた電子メールアドレス、名前、住所、電話番号が公開されることになります。これは犯罪の抑止力になると思われるかもしれませんが、効果的ではありませんでした。usTLD は悪用されることでよく知られています。

Krebs on Security が最近報告したように、usTLD は最も悪用されている国コード TLD（ccTLD）の 1 つであり、登録者と米国との関係は検証されていません。[13]Krebs は GoDaddy にレジストリとしての責任があるとしていますが、TLD は、2020 年に GoDaddy がレジストリの責任を引き継ぐ前に悪用されました。かつては高度に構造化され、管理されていた TLD でしたが、2002 年に Neustar が TLD の管理契約を獲得した後、第 2 レベルドメイン（SLD）の登録が可能になりました。[14]Infoblox は、他のすべての TLD と比較して、usTLD を中程度だがわずかに高いリスク（スコア 6）と評価しています。

NameSilo で .us ドメインを登録するには、電子メールアドレスと、5 つの Nexus カテゴリと申請目的のいずれかを選択する必要があります（下の図 4 を参照）。これらは、登録者と米国との関連性を確立するために使用されますが、承認基準は非常に広範囲です。[15] 登録プロセス中に、これらのうちの 1 つを満たしており、1 つを選択する必要があるという警告がユーザーに表示されます。この申請の目的要件は、個人の登録と組織の登録を分離します。

11 https://www.namesilo.com/support/v2/articles/domain-manager/dns-troubleshooting

12 https://www.about.us/faqs

13 https://krebsonsecurity.com/2023/09/why-is-us-being-used-to-phish-so-many-of-us/

14 https://en.wikipedia.org/wiki/.us

15 https://www.namesilo.com/popups/us_abbreviations.php

.US Abbreviations

Abbreviations to use when making API calls related to .US domains are listed below:

.US Nexus Categories

ABBREVIATION	
C11	US Citizen
C12	US Permanent Resident
C21	Incorporated or organized in US
C31	Foreign entity doing business in US
C32	Foreign entity with office in US

.US Application Purposes

ABBREVIATION	
P1	Business for Profit
P2	Non-Profit
P3	Personal
P4	Educational
P5	Governmental

図 *4. usTLD* 内のドメイン名の登録者は、上記のリストから関連する *Nexus* カテゴリと申請目的を選択する必要がある。この情報は、*WHOIS* レコードで公開される。

NameSilo でドメインの構成を完了させるには、登録者は名前、住所、電話番号も提供する必要がありますが、これらは検証されておらず、関連する WHOIS レコードは自動的に更新されません。更新を行わない場合、購入に関連付けられた電子メールアドレスのみが公開されます。登録者は連絡先情報を以前に購入したドメイン名に関連付けることを選択できますが、これはアカウント所有者の情報とは別の設定です。このプロセス全体が偽のデータで完了可能で、ドメインの代金をビットコインで支払うことができるため、脅威アクターは大きな困難もなくサービスを悪用できます。NameSilo はこの特定のケースで悪用されているレジストラですが、ここで取り上げた問題は業界全体で起こっています。

Prolific Puma ドメイン登録者はこれまで、営利目的 (P1) でドメインを使用する米国市民 (C11) であると主張してきましたが、このパターンは最近変化しています。**10 月 4 日から、usTLD 内の Prolific Puma のドメインが、既存登録と新規登録の両方を含む、個人使用 (P3) と個人登録設定のドメインに切り替わっていることを確認しました。**このアクティビティにより、Prolific Puma が悪意のあるアクターである疑いが排除されてしまいました。10 月中旬現在、usTLD 内の約 2000 の Prolific Puma ドメインが個人登録されています。

usTLD 内に個人登録が存在することは憂慮すべきことであり、usTLD の規約に違反しています。WHOIS データによる詳細情報の欠如は、過去数年間のインテリジェンスによる調査を妨げてきましたが、さらに重要なのは、NameSilo に関する私たち自身の経験から、インターフェースを介して usTLD 内のドメインの個人登録を選択することはできないということです。それにもかかわらず、実際には実行されました。もう少し深く掘り下げて、9 月 1 日から 10 月 15 日までに当社が処理したすべてのドメインを評価したところ、Prolific Puma が Privacy Guardian 保護下にある .us ドメインの大部分を占めていましたが、それだけではありませんでした。この期間中に usTLD について報告した 200 を超えるレジストラのうち、下の表に示すように、個人登録データに関連付けられていたレジストラは 4 つだけでした。**プライベートレコードを持つドメイン全体のうち、99% 以上が NameSilo** に登録されていました。現時点では、この事象には説明がついていません。

レジストラ	ドメイン数（2023 年 9 月 1 日〜10 月 15 日）
NameSilo – Prolific Puma	1062
NameSilo – おそらく Prolific Puma ではない	411
PorkBun	5
NameCheap	4
Sav.com	1

表 2. usTLD 内の個人登録ドメイン（レジストラ別）。これらは usTLD ポリシーに違反しています。

.us ドメイン名の制限基準は厳しいように思われるかもしれませんが、よく調べてみると、この TLD 内でドメインを登録できないのは完全な国外団体だけです。登録者が虚偽の WHOIS 情報を提供している疑いがある場合、Internet Corporation for Assigned Names and Numbers（ICANN）はレジストラに調査を要求し、情報の更新を許可します。[16]Nexus の要件ポリシーによれば、レジストラは登録者に不完全な情報や不正確な情報を更新するための 30 日間の猶予を与える必要があります。NameSilo と GoDaddy は、Nexus による認証よりも、悪意のあるアクティビティに基づいてドメインを削除しやすい立場にあります。しかし、Prolific Puma のような中間層にいる攻撃者の場合、具体的にはどのように対処すれば良いのでしょうか。

usTLD の悪用は、.xyz や .website など他のドメインの悪用と同様に、実際に起こっています。しかし、現代のプライバシー規制とテクノロジーにおいて、特に DNS の規模では、悪用と正当な使用を区別することは簡単ではありません。DNS の脅威アクターから消費者と組織を保護するには、業界の協力が必要です。当社としては、9 月に NameSilo と GoDaddy の両社に Prolific Puma の活動について通知しました。ただし、usTLD の要件に違反する可能性があることは別として、悪意のある目的で直接使用されていないドメインをレジストラが規制することは困難です。当社は、最近のドメインの大規模なコレクションを Spamhaus やその他のベンダーと共有しました。[17]

PROLIFIC PUMA の特徴

脅威アクターの本質は個人です。彼らの戦術、技術、手順(TTP) には、よく現れる癖があります。マルウェアの脅威アクターは、変数名の選択やコードへのコメント方法によって区別できる可能性があります。これらの選択は、彼らの興味、習慣、ユーモアのセンスを反映している可能性があります。DNS の脅威アクターも例外ではありませんが、一般的に DNS とドメイン登録レコードで扱うべき情報はほとんどありません。

Infoblox では、疑わしい悪意のある DNS アクティビティに重点を置いています。ドメイン名のリソースは DNS の脅威アクターによるものですが、その真の身元や場所を特定しようとすることはめったにありません。アナリストが仮想世界の活動を物理世界に結び付けようとするこの種の属性調査業務は、専門分野であり、時間がかかります。しかし、Prolific Puma は個人登録を許可していないレジストリである usTLD にドメインを登録しているため、そこに Prolific Puma の個性を垣間見ることができます。

16 https://www.icann.org/resources/pages/inaccuracy-2013-03-22-en

17 https://www.spamhaus.org/

可能な場合、Prolific Puma は個人のドメイン登録を使用しますが、usTLD での登録は公開する必要があります。これらのドメインでは、このアクターは Black Pumas の曲「October 33」の引用を含むメールアドレスを一貫して使用しています。[18] テキサス州オースティンを拠点とするサイケデリックなソウルバンドである Black Pumas は、2019 年にシングル「Colors」で名声を博しました。[19] この曲「October 33」はトップチャートには入らず、「Prolific Puma」と同様に謎が残っています。[20] 歌詞はわかりやすいラブレターでありながら、孤独について言及しており、意図的に耳に残るフィーリングを持つ音楽です。[21]2019 年にグラミー賞の最優秀新人賞にノミネートされたにもかかわらず、Black Pumas の名前は一般に浸透していません。Prolific Puma はLeila Puma という名前を使っています。この名前も、やはり Black Pumas を指して作られています。「Leila」という名前はアラビア語に由来し、「夜」を意味します。

Prolific Puma の現実での正体は分かりませんが、登録データから彼らの性質について興味深い洞察が得られます。Black Pumas とミステリアスな曲「October 33」への言及に加えて、Prolific Puma は個人用のウクライナの電子メールアドレスを使用しています。それらが提供する住所は、ポーランドの小学校で、どの工業都市にもあるような、これといった特徴のない建物です。ポーランドで 3 番目に大きい都市ウッチは、2022 年 2 月のロシアによる侵攻以来、ウクライナ難民を受け入れてきました。[22]Black Pumas による Kinks のカバー曲「Strangers」は、「Ukraine Strangers（見知らぬウクライナ人たち）」というタイトルの、ウクライナ難民をフィーチャーした感動的な YouTube 動画になりました。Prolific Puma の活動とは関係ありませんが、この動画は 2022 年秋に多くの視聴者に届きました。[23] 前述のように、登録者の情報は NameSilo によって検証されておらず、偽物のようですが、登録者の選択により、Prolific Puma を構成する単独または複数の人物について、ある程度の洞察が得られます。

PROLIFIC PUMA の運用

Prolific Puma は、ドメインの登録後、数週間そのドメインを未使用のまま、または保留中のまま放置しておくことがよくあります。この手法は、**戦略的エイジング**と呼ばれます。[24] フィッシング攻撃は、従来新しく登録されたドメインに結び付けられているため、多くのセキュリティシステムがそれらのドメインへのアクセスをブロックしています。これに対して、脅威アクターは、キャンペーンでドメインが使用するのを待ったり、ドメインを「古くする」ことで、多くのセキュリティ保護を回避できることに気付きました。

Prolific Puma は、エイジングプロセス中に少数の DNS クエリを行いますが、これは、脅威アクターがドメイン名に対する評価を得るために使用する方法です。この期間中、ドメインは NameSilo に保留されます。Prolific Puma は、ビットコインを使用して購入した、専用 IP アドレスを持つ仮想プライベートサーバー（VPS）上の防弾ホスティングプロバイダーにそれらを転送します。しばらくすると彼らはドメインを放棄し、DNS レコードが専用 IP アドレスを指したまま放置することがわかりました。

私たちがこれまで見てきた運用手法の幅広さから、Prolific Puma は他者のためにサービスを提供しており、最終的なランディングページは彼らの管理下にはないものと思われます。しかし、同じ脅威アクターが、リンク短縮サービスと、それを介して行われるすべての悪意のあるアクティビティ

18 https://www.blackpumas.com/

19 https://en.wikipedia.org/wiki/Black_Pumas

20 https://www.youtube.com/watch?v=an3AkQL62F8

21 https://www.facebook.com/theblackpumas/videos/black-pumas-oct-33-song-breakdown/461719384620852/

22 https://eurocities.eu/latest/ukrainian-refugee-integration-in-lodz-and-timisoara/#:~:text=The%20city%20of%20Lodz%20in,refugees%20since%20the%20Russian%20invasion

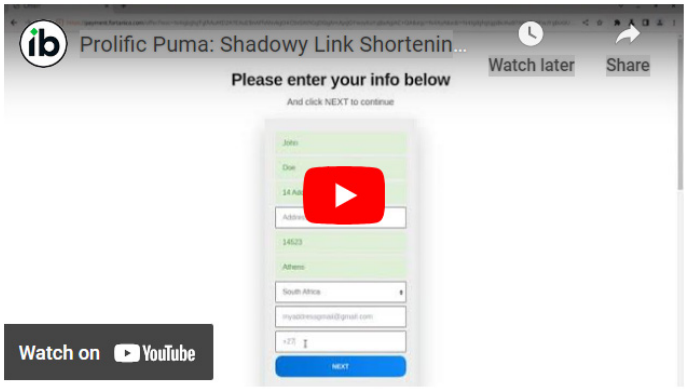
23 https://www.youtube.com/watch?v=D_Ap_7wjHIs

24 https://heimdalsecurity.com/blog/aged-domains-the-silent-danger-to-cybersecurity-new-report/

の両方をコントロールしている可能性も残っています。Prolific Puma がどのようにサービスを宣伝しているのか、ユーザーがどのように短縮 URL を受け取っているのか、合法的なトラフィックがあるのかどうかについて、当社は明らかにしていません。Prolific Puma のサービスを介したキャンペーンでは、他の DNS 脅威アクターが管理するドメインの大規模なネットワークが見つかっており、多くの場合、NameCheap などの安価なレジストラで登録されています。これらのキャンペーンドメインには、RDGA によって生成されているものもあります。

キャンペーン例

Prolific Puma は、さまざまなフィッシング、詐欺、マルウェアのアクティビティのためにリンク短縮ツールを運営しています。以下では、このツールが利用されているキャンペーンの 1 つを例として説明します。図 5.1 ～ 5.4 は、被害者が最初に短縮リンク（`http://bwkd[.]me/ZFjfA3`）をクリックした後に表示される画面のスクリーンショットです。このリンクは、電子メールに似せて設計されたフィッシングページに接続し、ユーザーに個人情報を提供して支払いを行うよう促します。その後、ブラウザープラグイン・マルウェアに感染させます。以下に、このプロセスについて記録した画面録画を示します。



このキャンペーンにおける、短縮リンクからブラウザプラグイン・マルウェアまでの技術的な手順は次のとおりです。

- 最初の短縮リンク `http://bwkd[.]me/ZFjfA3` が、次の URL にリダイレクトする。
- リダイレクトされた `http://ksaguna[.]com/click.php?key=<redacted>` から、さらに次のページにリダイレクトする。
- `https://www[.]asdboloa[.]com/ZA/AB_zagopb/?uclick=<redacted>`
  - » この最後のウェブサイトは、新しい iPhone 15 をテストするチャンスを獲得したことをユーザーに伝える、偽の Gmail メッセージ。
- ユーザーは、携帯電話を受け取るには、リンク（`https://www[.]game[.]co[.]za/2023program`）をクリックして配送情報を入力するよう指示される。ウェブサイト（`www[.]game[.]co[.]za`）は、消費者を引き付けるためにプロモーション活動を行っている南アフリカのディスカウント小売業者です。
- 適切な条件でこのリンクをたどると、トライアルに参加するために 18 南アフリカランド（ZAR）を支払うように求められます。
- そこから、ユーザーには郵便物追跡と表示されたページが表示され、`fubsdgd[.]com` からの通知を承認するよう促されます。[受け入れる] をクリックすると、OneSignal サービスを使用してプッシュ通知を行うブラウザマルウェアのインストールが開始されます。ブラウザプラグイン・マルウェアは一般的に広告に関連付けられますが、私たちの経験では、広告とともにスパムメール、フィッシング、およびその他のマルウェアを配信するためによく使用されます。
- 最後に、被害者は一連のプロンプトに誘導され、配送設定の確認と個人情報の入力を求められます。

元の短縮 URL がどのようにして被害者に届けられるのかは不明ですが、偽の Gmail メッセージが開くことから、SMS テキストメッセージ経由で届けられる可能性があります。被害者へのエクスプロイト中に使用されたドメインは変化し、それ自体が大規模なネットワークの一部となっています。このキャンペーンでは、各ステップで他の「参加者」からの推薦レビューが積極的に提供されるなど、さまざまな手法を使用して、被害者にオファーが本物であることを確信させます。

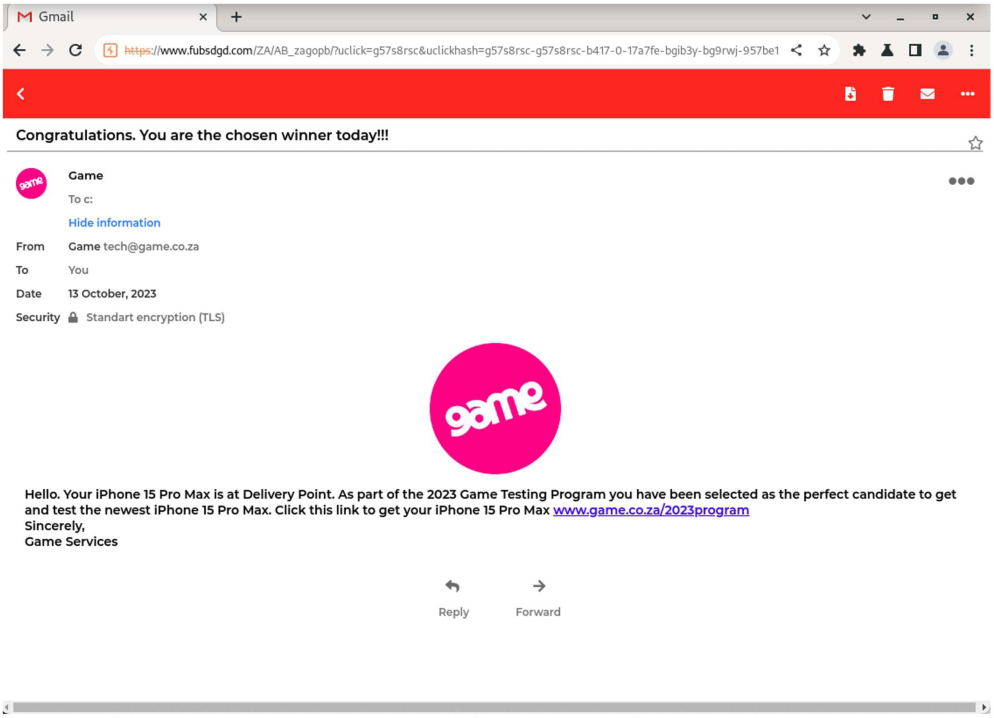


図 5.1：*Prolific Puma* リンク短縮サービスによって配信されるコンテンツの例。元の短縮リンク（*http://bwkd[.]me/ZFjfA3*）からリダイレクトされ、最終的には *Gmail* から配信される電子メールと似せて作られたフィッシングページにつながる。

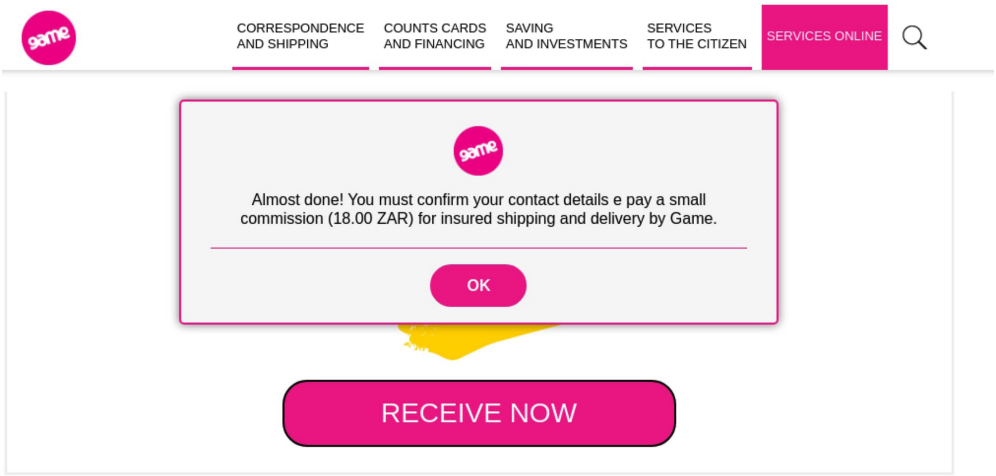


図 5.2. キャンペーンで詐欺と個人情報の盗難が行われる部分。図 *5.1* のように、無料の *iPhone* を受け取ることを選択すると、ユーザーは料金を支払い、名前と住所を入力するよう求められる。

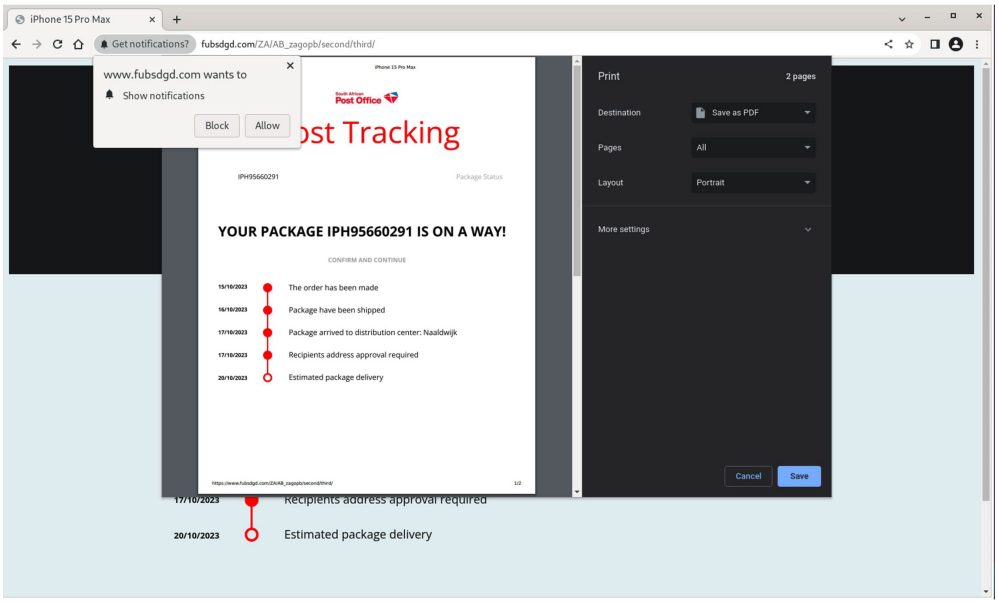
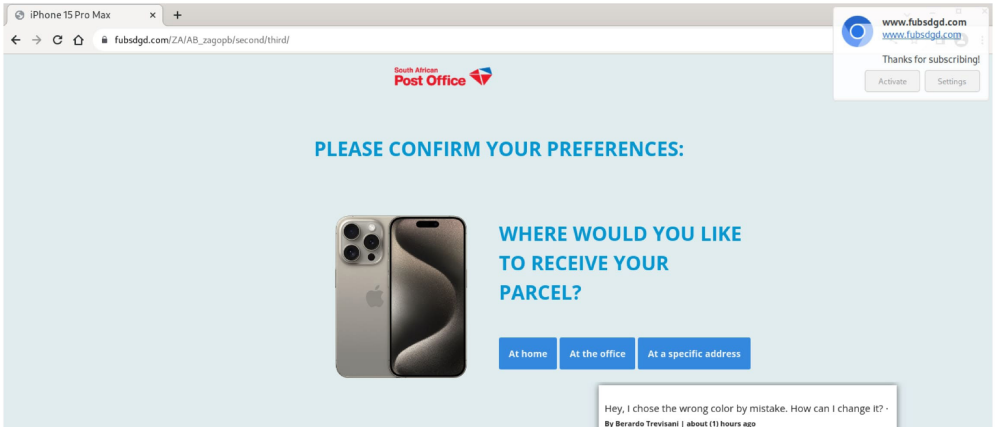


図 5.3. キャンペーンのマルウェア配信部分。被害者が図 5.2 に示す料金を支払うと、郵便物配達通知が届き、*fubsdgd[.]com* からの通知を提示するよう求められる。通知を受け入れると、マルウェアが被害者の端末に送信される。



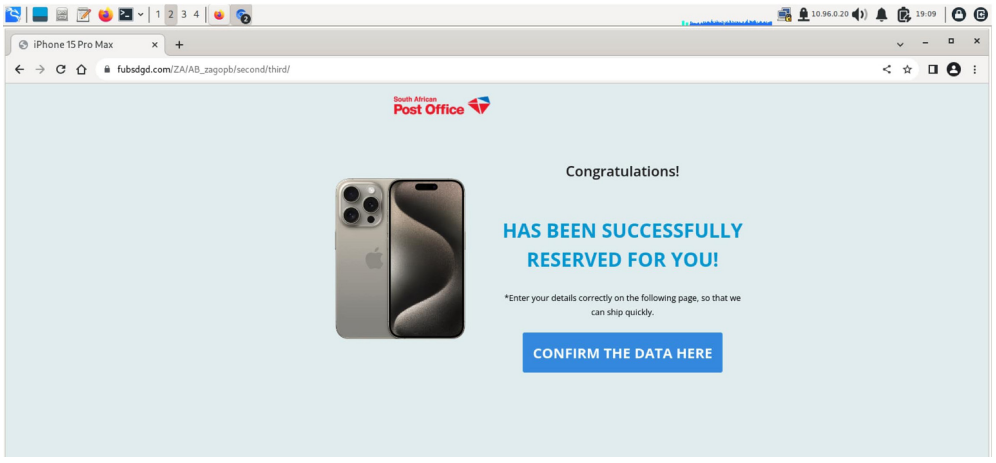


図 5.4*a* ～ *b*. 図 5.3 に示す通知を承諾すると、ユーザーは一連の画面でさらに詳細と設定を入力するよう求められる。

結論

Prolific Puma は、DNS が犯罪活動を支援するために悪用が可能であり、何年もの間検知されないままである実態を示しています。サプライチェーンの一部であるこのアクターは、検出や撃退が困難です。従来のセキュリティシステムは、リンクの最終的なランディングページに基づいてユーザーを被害から保護します。しかし、DNS Detection and Response のシステムは、Prolific Puma や同様のサービスプロバイダを妨害することができ、それによってフィッシング、スパムメール、マルウェアを配信するためにそれらに依存しているすべてのアクターを阻止することができます。RDGA と安価なドメインレジストラを使用することで、Prolific Puma は事業規模を拡大し、持続させることができます。しかし同時に、DNS とドメイン登録記録から、当社は RDGA の使用を検出することもできます。

Prolific Puma は、Infoblox が発見したリンク短縮サービス運営者の 1 つに過ぎず、リンク短縮サービスは影の経済で暗躍するサービスの 1 つにすぎません。**ほとんどの場合、DNS 脅威アクターは、新規登録、構成、またはクエリされた疑わしいドメインを特定する分析を通じて最初に発見されます。**ドメインと悪意のあるアクティビティを相関させる前であっても、TLD やネームサーバーの評価などの他の機能を使用して、関連するドメインを疑わしいものとしてフラグ付けできます。その後、ドメインを関連付けて脅威アクターを隔離できます。疑わしいドメインへのアクセスをブロックすることで、組織はネットワークとユーザーに対して非常に効果的で、後悔の少ない、セキュリティの高いポリシーを実装できます。

アクティビティの指標

以下は、Prolific Puma とそれらが促進するキャンペーンに関連する指標の極一部です。最近の指標のより包括的なリストは、こちらにある当社のオープンな GitHub リポジトリでご覧ください。

アクティビティの指標	指標の種類
hygmi[.]com	Prolific Puma リンク短縮サービスによるドメイン
yyds[.]is	
0cq[.]us	
4cu[.]us	
regz[.]info	
u5s[.]us	
1jb[.]us	
jrbc[.]info	
uhje[.]me	
0md[.]us	
fh3[.]us	
0qa[.]us	
9jw[.]us	
iv0[.]us	
od9[.]us	
rpzp[.]me	

アクティビティの指標	指標の種類
8fx[.]us	
3vb[.]us	
r1u[.]us	
zost[.]link	
9ow[.]us	
sf8i[.]us	
bu9[.]us	
ce2[.]us	
wf6[.]us	
v8z[.]us	
zj4[.]us	
rjvb[.]link	
fssu[.]link	
xbsf[.]link	
wqeh[.]link	

アクティビティの指標	指標の種類
ymql[.]link 7tz[.]us w6q[.]us giqj[.]me u3q[.]us ke0[.]us v1u[.]us ti7[.]us 2zc[.]us gf6[.]us 6dr[.]us 6or[.]us kc0[.]us 0ty[.]us styi.info 6fe[.]us u8n[.]us d6s[.]us	
v8z[.]us zj4[.]us rjvb[.]link fssu[.]link xbsf[.]link wqeh[.]link ymql[.]link 7tz[.]us	リンク短縮サービスのホスティング IP

アクティビティの指標	指標の種類
bwkd[.]me ksaguna[.]com asdboloa[.]com game.co[.]za	リダイレクトとランディングページ
fubsdgd[.]com	ブラウザプラグイン・マルウェアのドメイン
blackpumaoct33@ukr[.]net	Prolific Puma の登録メールアドレス

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大手企業であり、数多くのアグリゲーター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：20241008v1