infoblox

Threat Intel

MUDDLING MEERKAT：GREAT FIREWALL 操作の巧者

作成者
Dr. Renée Burton
と匿名

目次

エグゼクティブサマリー

本稿では、中華人民共和国（PRC）の国家主体と思われる不可解なアクターである「Muddling Meerkat」を紹介します。Muddling Meerkat は、大量の広範囲に分散されたクエリを作成し、その後オープン DNS リゾルバーを使用してインターネットを通じて伝播させることで、DNS を介してアクティブな操作を実行します。その活動は、中国と中国のアクターと密接に関連する 2 つのトピックである、「中国の Great Firewall（GFW）」と「スロードリップ」、つまりランダムプレフィックス分散型サービス拒否(DDoS)攻撃と絡み合っています。Muddling Meerkat の活動は一見 DNS DDoS 攻撃のように見えますが、少なくとも短期的にはサービス拒否が目的である可能性は低いようです。Muddling Meerkat の活動は長期にわたり（2019 年 10 月に開始されたようです）、DNS に関する高度な専門知識を示しています。

Muddling Meerkat の活動は複雑です。実際、あまりにも複雑なため、Muddling Meerkat は脅威ではないと思われるかもしれません。しかし、サイバーセキュリティ、特に DNS の複雑な世界では、戦略的に考える必要があります。2024 年 2 月、米国サイバーセキュリティ・インフラセキュリティ庁（CISA）と複数の国際パートナーは、「近年、米国のサイバー脅威活動は、スパイ活動に焦点を当てたものから、米国の重要インフラに対する破壊的なサイバー攻撃の可能性に備えるための事前準備へと戦略的にシフトしている」という勧告を発表しました。[1] この具体的な勧告は、Volt Typhoon というアクターが使用した「土地に依存しない生活」のテクニックに焦点を当てたものでしたが、「PRC のサイバーアクターは、通常のシステムやネットワークの活動に紛れ込み、ネットワーク防御による識別を回避し、一般的なロギング構成でキャプチャされる活動量を制限する」というメッセージは、Muddling Meerkat がいかにうまく隠されているかに不気味なほど似ています。[2]

MUDDLING MEERKAT とは

Muddling Meerkat は GFW を制御する能力を持っているようで、これまで報告されていない方法でそれを実行します。彼らの活動の一部は「スロードリップ」攻撃と似ていますが、Muddling Meerkat の動機と目的は不明です。データによると、その活動は次のことをおこなっています：

- 中国の IP 空間にあるサーバーを利用して、世界中の IP アドレスに対してランダムなサブドメインの DNS クエリを行い、キャンペーンを実施することで、最終的には世界的に DNS ネットワークの調査を実行
- 攻撃者の制御下にない .com および .org のトップレベルドメイン（TLD）に属する一連のドメインについて、短いランダムホスト名を対象に MX レコードクエリやその他のレコードタイプを使用
- GFW によって注入された中国の IP アドレスから偽の MX レコードを誘導
- DNS ブロックリストを避け、多くの企業の Active Directory ドメインと衝突しないように、通常は 2,000 年以前に登録された「超経年」ドメインを使用
- 現在のステータスや所有権ではなく、その長さと築年数に基づいて、悪用されるドメインを選択：ドメインの多くは放棄されたり、疑わしい用途に転用されたりしていますが、合法的な団体によって積極的に使用されているものもあります
- 1 ～ 3 日間のキャンペーンをほぼ継続的に実施
- 送信元 IP アドレスを大規模にスプーフィングしているようには見えず、代わりに専用サーバーから DNS クエリを開始
- 検出やサービスの中断を避けるためにサイズに制限あり
- 個別のコンポーネントで実行され、時間の経過とともに異なる DNS パターンが作成される可能性あり

1 https://www.linkedin.com/posts/cisagov_with-us-and-international-government-partners-activity-7161082451354603520-pv0q

2 https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques

- 2019 年 10 月 15 日頃に開始 [3]

現在私たちが理解している Muddling Meerkat の活動を簡略化して図 1 に示します。

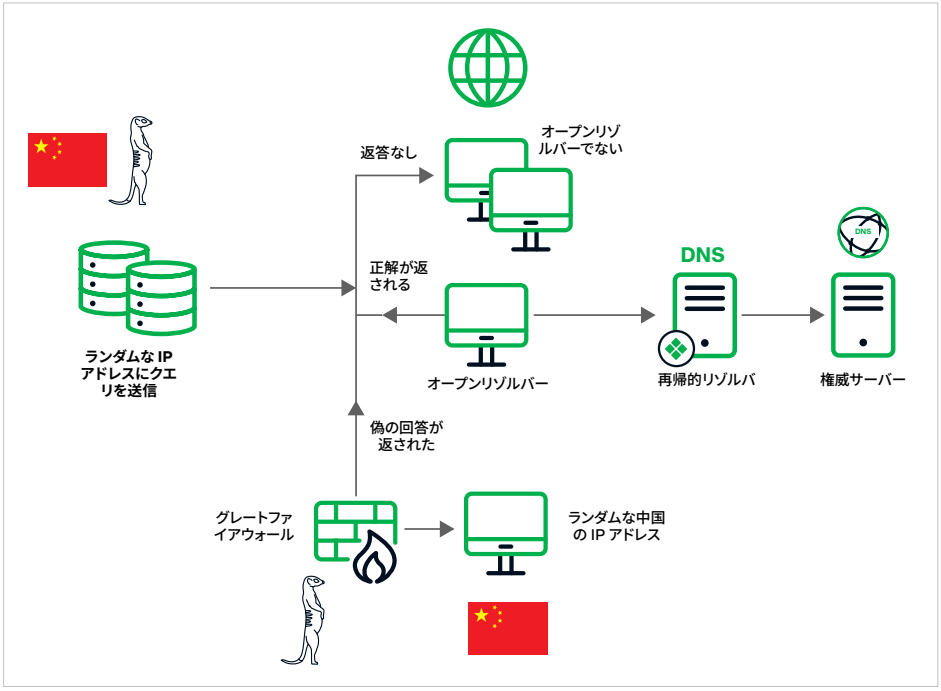

図 1 現在わかっている Muddling Meerkat の活動の概要。Great Firewall は、MX クエリに対して偽の回答を提供することが確認されています。この動作は、これまで文書化されていません。

私たちが Muddling Meercat を発見したのは偶然でした。複数の組織のデータの可視性がなければ、アクターはもっと何年も発見されなかったかもしれません。このレポートは、非公開の脅威研究者やセキュリティベンダー、ミシガン州の公立大学が運営する独立非営利法人 Merit Network、および DomainTools との共同研究です。[4] コントリビューターはそれぞれ、何らかの形でパッシブ DNS コレクションにアクセスでき、独自の視点から Muddling Meerkat を観察できます。Muddling Meerkat の活動全体を 1 つの視点から観察することは不可能です。情報を組み合わせることで、単独では不可能な行為者の活動の全体像を把握できます。この論文内の各調査結果は、特に明記されていない限り、2 つの独立したソースで確認されているか、Infoblox DNS リゾルバーから直接抽出されたものです。

背景

私は、一人称で書くという異例の方法でこのレポートを書いています。部分的には、このような奇妙なストーリーを語るときには一人称の方が適切であるように思われたのです。さらに、中国の DNS 脅威アクターに関する私のこれまでの研究と出版物は、Muddling Meerkat に関する私の結論を導くのに役立ちました。私のキャリアの初期に、国家安全保障局（NSA）の同僚と私は、数年にわたって DNS ベースの DDoS 攻撃を行う中国のアクターを何千時間もかけて研究しました。私たちはそのアクターを ExploderBot と名付け、2018 年の春にその結果を静かに公開しました。ExploderBot は 2014 年以来ほぼ毎日稼働し、インターネットサービスプロバイダーに大混乱をもたらしていましたが、私たちの論文が発表されてからわずか 1 か月後に稼働を停止しました。彼らは 2018 年 5 月 18 日以来、姿を消しています。中国の DNS DDoS 攻撃の性質が変化し、私は 2020 年後半にその変

3　作戦が数か月早い 2019 年 6 月に開始されたという証拠はいくつかありますが、この日付は確認できていません。

4　https://www.merit.edu/

化に関する長期研究を執筆しました。それ以来、私は中国によるものであろうとなかろうと、DNS DDoS 攻撃を調べることにあまり時間を費やしていません。Infoblox には、アクティビティの兆候を探し、高度な　DNS 保護（ADP）製品の顧客に関連するドメインを自動的にブロックする検出器がありますが、そのシステムは主に人間の介入を必要せず機能します。

Muddling Meerkat は、違法な中国のギャンブルや偽のアプリを扱う他の脅威アクターにサービスを提供する DNS 脅威アクターを調査している際、私の目に留まりました。目立ったのはギャンブルではなく、DNS メールサーバー（MX）レコードに対する異常なクエリと応答でした。Muddling Meerkat では他のレコードタイプも使用されていることがわかりましたが、DNS 内での MX レコードの特殊な性質により、より明確な分析が可能になるため、このレポートでは MX レコードに焦点を当てます。

GFW は、中国政府が不適切または違法とみなすウェブサイトやサービスに中国居住者がアクセスするのを防ぐ目的で機能します。[5] しかし、DNS クエリに誤った回答を挿入することも知られています。GFW は、中国の IP 空間に出入りするすべての IP トラフィックに適用されます。後ほど「中国の Great Firewall の調査」のセクションで示すように、GFW の誤った回答の動作は簡単に実証が可能です。GFW は「サイドオペレーター」と表現でき、DNS レスポンスを直接変更するのではなく、独自のレスポンスを注入し、元の意図した宛先からのレスポンスと競合状態になります。GFW 応答が最初に要求者によって受信されると、DNS キャッシュが汚染される可能性があります。中国は GFW に加えて、グレートキャノン（GC）と呼ばれるシステムを運用しています。GC は「中間オペレーター」であり、宛先への途中でパケットを変更することができます。[6]GC は、大規模な DDoS 攻撃に使用されてきました。2015 年には、GFW での検閲を監視する非政府組織 GreatFire.org への攻撃に使用されました。[7] それ以来、香港の抗議活動を阻止することを目的とした攻撃を含む DDoS 攻撃に断続的に使用されています。[8]GC オペレーターの実際のスコープは不明です。GFW と GC を組み合わせると、大量のノイズと誤解を招くデータが生成され、DNS の異常な動作の調査を妨げる可能性があります。私は個人的に数多くのトレイルを探し回りましたが、結局「これは単に GFW なのだ」という結論に至りました。

Muddling Meerkat は、MX レコードの悪用に加えて、ボリュームは少ないものの DNS DDoS 攻撃と同様の動作パターンを示したため、私たちの注目を集めました。スロードリップ、またはランダムプレフィックスである DNS DDoS 攻撃では、ターゲットドメインの明らかにランダムなサブドメインへのクエリが大規模に行われ、通常はオープンリゾルバーを介して伝播されます。これらの攻撃はもともと 2014 年に発生し、最初に報告された被害者は中国人でした。私と数人の同僚は、これらの攻撃の複数年にわたる DNS ログを調査し、実証可能な損害をもたらした攻撃のほとんどが ExploderBot という単一の攻撃者によって実行されたという結論に達しました。私たちは、ExploderBot の DNS クエリと IP パケットに、5 年間にわたって一貫している複数の数学的アーティファクトを特定しました。また、偽装された送信元および宛先 IP アドレスを含む ExploderBot からのトラフィックが、インターネットバックボーンの近くに挿入されたことも判明しました。クエリを受け取ったオープンリゾルバーは、それを独自の再帰リゾルバーに転送します。未知のオープンリゾルバーを含む管理対象外のデバイスがたくさんあるネットワークでは、クエリの量がインターネットサーバープロバイダーに混乱をもたらします。ExploderBot DNS クエリで使用された偽装 IP アドレスは広範囲に配布されており、GFW 応答は長い間、私たちの分析を妨げる誤報として機能していました。ExploderBot の活動が 2018 年 5 月に停止したとき、残ったのは、明らかな影響や目的がほとんどない、継続的な低ボリュームの奇妙なでした。過去数年間、ランダムプレフィックス攻撃がネームサーバーにある程度定期的に影響を及ぼしてきましたが、ExploderBot と同じボリュームレベルは見たことがありません。[9]

5 https://www.cybereason.com/blog/malicious-life-podcast-the-great-firewall-of-china-part-1

6 https://citizenlab.ca/2015/04/chinas-great-cannon/

7 https://foreignpolicy.com/2015/04/10/great-cannon-china-internet-cyber-attack-baidu/

8 https://cybersecurity.att.com/blogs/labs-research/the-great-cannon-has-been-deployed-again

9 https://infosec.exchange/@ricci@discuss.systems/111508151184559310

この論文では、GFW について私が知っていることを踏まえて Muddling Meerkat の活動について説明し、その活動を検出する方法を説明し、Muddling Meerkat のようなアクターを分析しようとする際の落とし穴について説明します。特に、オープンリゾルバーの危険性と、DNS または Microsoft Active Directory での未登録の検索ドメインの使用について読者に警告したいと思います。これは、DDoS 攻撃への参加とネットワーク情報の敵への漏洩の両方につながる可能性があります。

ちょっとした専門用語

DNS の言語はわかりにくいものです。IP パケットと組み合わせると、さらにわかりにくくなります。この研究の過程で、私と共著者は何度も立ち止まって自問しなければなりませんでした―「ここで私たちが話している IP とはどんな IP なのだろう?」と。論文全体を通して、いくつかの用語を次のように使用していますのでご覧ください。

- DNS クエリを作成する、または DNS クエリの応答を受信する IP アドレスは**「クエリア IP アドレス」と呼ばれます**。この名前は、IP パケットにクエリまたは応答が含まれていたかどうかによって適用されます。
- DNS クエリに応答する IP アドレスは**「レスポンダ IP アドレス」と呼ばれます**。理想的な世界では、これらはリゾルバーですが、Muddling Meerkat による「中国の IP アドレスの役割」というセクションでは、後ほど説明しますが、これらは単なる IP アドレスです。
- 応答の DNS リソースレコードに含まれる IP アドレスは、**「解決 IP アドレス」と呼ばれます**。
- 私が応答で DNS リソースレコードについて一般的に話す場合、**答えは**レコードに含まれる値を指していると言うかもしれません。

MUDDLING MEERKAT の活動

Muddling Meerkat の活動は複雑で、攻撃者が DNS を熟知しているだけでなく、インターネットに精通していることを示しています。説明を簡素化するために、私は、DNS MX レコードまたは MX 解決チェーンに関連する活動のコンポーネントのみを取り上げます。いずれの場合も、アクターの管理下にない登録済みドメインがあり、これを**ターゲットドメイン**と呼びます。このレポートでは、次の 3 種類の活動について説明します。

- ターゲットドメインの MX レコードのクエリ
- ターゲットドメインのランダムなホスト名の MX レコードのクエリ
- ターゲットドメインのランダムなホスト名の A レコードのクエリ

ターゲットドメインのランダムなホスト名のクエリは、スローディップ DDoS 攻撃の典型ですが、Muddling Meerkat クエリは、ExploderBot やその他のスローディップ攻撃のクエリとは異なります。ホスト名は短く、さらに、一部のスロードリップ攻撃にはさまざまなクエリタイプが含まれていますが、最も一般的なタイプは依然として IPv4 アドレスの A レコードです。私はこれまで、Muddling Meerkat の特徴となるタイプの MX レコードアクティビティを見たことはありません。ターゲットドメインの選択も重要です。後ほど「Muddling Meerkat のターゲットドメイン」セクションでご説明します。

Muddling Meerkat という名前について：ミーアキャットはマングース科に属します。見た目はかわいらしいですが、小さい体とは裏腹に賢く、勤勉で、非常に獰猛です。Muddling Meerkat は、MX DNS レコードを悪用し、中国のグレートファイアウォールに関連する操作を実行し、分析を妨害する混乱と誤報を加えることで知られています。操作にはオープンリゾルバーが広く使用されているため、活動は時間や場所によってまるでミーアキャットが巣穴から顔を出したり引っ込めたりするように、「現れたり消えたり」します。

中国の GREAT FIREWALL の調査

GFW は、Muddling Meerkat データにおいて重要な役割を果たしています。特定の DNS データコレクションにおいて、DNS クエリに対する誤った応答が観測されるためです。偽の応答を見ると、そのレコードのソース IP は中国の IP アドレスであり、GFW によるインジェクションまたは GC による修正と一致します。中国は米国に次いで、世界中に地理的に分散した 3 億 5000 万以上の IP アドレスを管理しています。この IP 空間に出入りするすべてのトラフィックに対して、GFW は非公開の意思決定に基づきユーザーのパフォーマンスに影響を与えることなく DNS クエリへの回答を挿入できます。これをうまく行うには、多くの専門知識が必要です。中国は世紀の変わり目に欧米のテクノロジー企業を活用してファイアウォールのコンポーネントを構築し、さまざまな監視メカニズムを実装し、そうすることで独自の能力と知識を構築しました。[10]

中国は、DNS ファイアウォールが一般的に使用する NXDOMAIN やその他の応答メカニズムを単に使用するのではなく、偽の回答で応答するシステムを設計しました。[11] これを聞いて私の言うことを鵜呑みにする必要はありません。ファイアウォールを自分で調べることができます。研究者は以前、数十万のドメインで誤った応答を発見し、これらの応答の一部が特定の再帰リゾルバーのキャッシュを汚染したと結論付けました。[12]ExploderBot に掲載された調査でも、それ以降の調査でも、GFW からの IP アドレスの応答はめまぐるしいものでした。

GFW の影響を示す最も簡単な方法は、確立された DNS サーバーではないランダムな中国の IP アドレスに DNS クエリを実行することです。Stephen Bortmeyer 氏は 015 のブログでこれについて説明しています。[13] 実験は、dig ユーティリティまたはオンラインツールを使用してコマンドラインから実行できます。一般的なドメインの A レコードを要求すると、DNS サービスをホストしていないにもかかわらず、中国の IP アドレスは必ず応答を返します。下の図 2 は、China Unicom に割り当てられ、現在サービスをホストしていない IP アドレスが、google[.]com の IP アドレスの DNS クエリに偽の応答を返す例を示しています。

```
; <<>> DiG diggui.com <<>> @111.193.204.201 google.com A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54398
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             60      IN      A       93.46.8.90

;; Query time: 214 msec
;; SERVER: 111.193.204.201#53(111.193.204.201)
;; WHEN: Tue Jan 09 00:15:06 UTC 2024
;; MSG SIZE  rcvd: 54
```

図 2。サービスをホストしていない China Unicom の IP アドレスが、google[.]com の A レコード DNS クエリにイタリアの IP アドレスで応答します。この応答は意図的なリダイレクトであり、応答ごとに変化します。画像提供：diggui[.].com。

10 https://www.cybereason.com/blog/malcious-life-podcast-the-great-firewall-of-china-part-1

11 https://citizenlab.ca/2021/11/gfwatch-a-longitudinal-measurement-platform-built-to-monitor-chinas-dns-censorship-at-scale/

12 How Great is the Great Firewall? Measuring China’s DNS Censorship. Nguyen Phong Hoang, et al., 30th USENIX Security Symposium (USENIX Security 21), https://www.usenix.org/system/files/sec21-hoang.pdf（最終アクセス日 2024 年 1 月 9 日）

13 https://www.bortzmeyer.org/sichuan-pepper.html

GFW が検閲手段として偽の応答を送信するドメインをどのように選択するかは不明です。検閲されていないドメインに対して同じ中国の IP アドレスを照会すると、通常、サーバーに到達できないというエラーが発生します。この結果は、GFW が特定のクエリに対してのみ回答を挿入することを示しています。私の経験では、GFW は、要求されたリソースの種類に関係なく、すべての DNS クエリに IPv4 アドレスで応答します。例えば、同じ IP アドレスに google[.]com の MX レコードを要求すると、今度は Korea Telecom に割り当てられた別の IPv4 アドレスが返されます。適切な MX レコードには、IPv4 アドレスではなく、完全修飾ドメイン名（FQDN）を含むテキスト文字列が含まれている必要があります（図 3 を参照）。TXT レコードまたはその他の非 A レコードタイプを照会すると、同様に IPv4 アドレスが返されます。他の研究者は 2021 年に GFW に関する大規模な縦断的研究を実施し、同じ結論に達しました。[14] その 1 年前には、別の研究者が CNAME レコードのインジェクションを 1 回報告しましたが、その反応については説明していませんでした。[15]

```
; <<>> DiG diggui.com <<>> @111.193.204.201 google.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62080
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      MX

;; ANSWER SECTION:
google.com.             60      IN      A       59.24.3.174

;; Query time: 208 msec
;; SERVER: 111.193.204.201#53(111.193.204.201)
;; WHEN: Tue Jan 09 00:25:37 UTC 2024
;; MSG SIZE  rcvd: 54
```

図 3。China Unicom の IP アドレスは、google[.]com の MX クエリに応答してランダムな IPv4 アドレスを返します。正しい応答は、メールサーバーの FQDN を返します。画像提供：diggui[.]com。

これらの実験は、GFW が通常どのように動作するかを直接示しています。選択的にインジェクションを実行します。特定のドメイン名に対する DNS 応答で、誤解を招くような回答がランダムに返されます。偽のパケットを挿入すると、要求されたレコードタイプに関係なく、常に IPv4 アドレスが返されます。一方、Muddling Meerkat は、中国の IP アドレスから適切にフォーマットされた偽の MX レコードを提供します。

ターゲットドメインの MX レコード

Muddling Meerkat の最も注目すべき特徴は、中国の IP アドレスからの偽の MX レコード応答が存在することです。これまで発表されたことのないこの行動は、GFW の標準的な行動とは異なります。これらの解決策は、DNS サービスをホストしていない中国の IP アドレスから発信されており、GFW と一致する偽の回答が含まれています。しかし、GFW の既知の動作とは異なり、Muddling Meerkat の MX レスポンスには IPv4 アドレスではなく、適切にフォーマットされた MX リソースレコードが含まれています。この特徴は実に驚くべきものであり、ほとんど説明のつかないものです。

このレポートでは、Muddling Meerkat の多くのターゲットドメインの 1 つである kb[.]com. を使用して、そのアクティビティを説明します。Muddling Meerkat の MX 回答レコードは、応答のソースが DNS リゾルバーではなくランダムな中国の IP アドレスであるため、通常の DNS 解決チェーンの外部で収集されたデータでのみ確認できます。Infoblox データは当社の再帰リゾルバーから取得されるため、分析用のデータを取得するために他のベンダーと提携しました。

14 How Great is the Great Firewall? Measuring China’s DNS Censorship. Nguyen Phong Hoang, et al., 30th USENIX Security Symposium (USENIX Security 21), https://www.usenix.org/system/files/sec21-hoang.pdf（最終アクセス日 2024 年 1 月 9 日）

15 Anonymous, et al. Triplet Censors: Demystifying Great {Firewall{\textquoteright}s} {DNS} Censorship Behavior, 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20), https://www.usenix.org/conference/foci20/presentation/anonymous（最終アクセス日 2024 年 1 月 9 日）

ある第三者は、2024 年 1 月下旬までの 120 日間にわたって、ドメイン kb[.]com の MX リソースレコードを含む DNS クエリ応答データを提供しました。具体的には、各ログには、kb[.]com の MX レコードに対する DNS クエリと、2 つのリソースレコードを含む応答が含まれていました。リソースレコードは適切にフォーマットされており、kb[.]com のランダムなホスト名（通常は 3 ～ 6 文字）を含む FQDN が含まれていました。このような MX レコード値の例は次のとおりです：

- pq5bo[.]kb[.]com
- uff0h[.]kb[.]com
- biuti[.]kb[.]com
- 8jxg1x[.]kb[.]com
- 8p0[.]kb[.]com

MX レコードに詳しくない方のために説明すると、これらの応答は kb[.]com のメールサーバーの FQDN になります。ネットワーク上のユーザーから kb[.]com ネットワーク内の受信者にメールを配信するには、2 つの DNS クエリが必要です。1 つ目は受信者のメールドメイン（ここでは kb[.]com）の MX レコード用で、2 つ目は MX レコード内に含まれる FQDN の IP アドレス用です。IP アドレスが取得されると、Simple Mail Transport Protocol（SMTP）サーバーはユーザーに代わってメールを送信できます（図 4 を参照）。

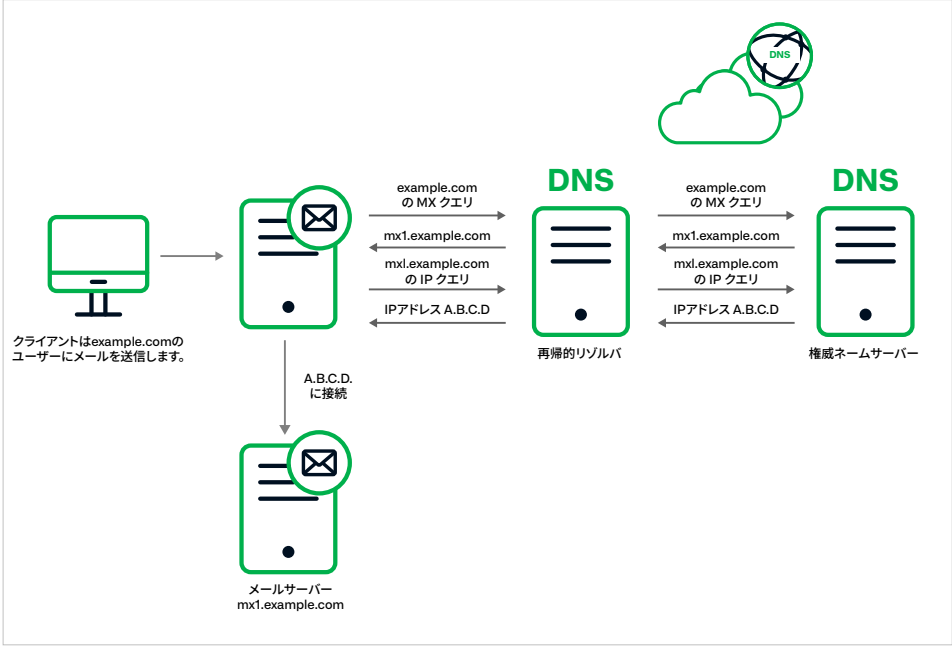

図 4 。メールサーバーの IP アドレスを見つけるための一般的な DNS 解決プロセス。メールサーバーの標準的な解決では、MX レコードと A レコードの両方に対するクエリが行われます。

サードパーティのデータでは、適切にフォーマットされた MX レコードは、DNS サーバーをホストしていないランダムな中国の IP アドレスから取得されています。さらに、これらの答えは一見正しいように見えますが、間違っています。ドメイン kb[.]com は現在、IBM の一部である権威ネームサービスである NS1 を使用して、中国に権威ネームサーバーを持っています。これらの権限のあるネームサーバーは、kb[.]com の MX レコードクエリに対して応答を返しません。したがって、中国の IP 空間から送信された DNS 応答は、通常の GFW の動作とは異なり、誤りであることが確認できます。

サードパーティのデータには、数件でなく数千件ものMXレコードが含まれていました。この期間中、履歴MXレコードセット内のすべてのホスト名が1日に表示され、合計で8,000件を超える一意のFQDNが記録されました。2番目のベンダーも同様の観測結果を示しています。回答には短いホスト名が含まれており、重複していません。その量は注目に値しますが、かなり小さく、DDoS攻撃に効果的であるには小さすぎます。ここでの答えが間違っているだけでなく、クエリ自体も疑わしいと考えられます。ドメインkb[.]comはかつて米国のマーケティング会社に所有されていましたが、現在はジオフェンスされた中国語のギャンブルをホストしています。クライアントがドメインにメールを送信する理由はなく、特にランダムな中国のIPアドレスから解決を要求する理由もありません。図5に示すように、サンプルには毎日MX分解能がありますが1日あたり100件以上のオブザベーションはほとんどありません。

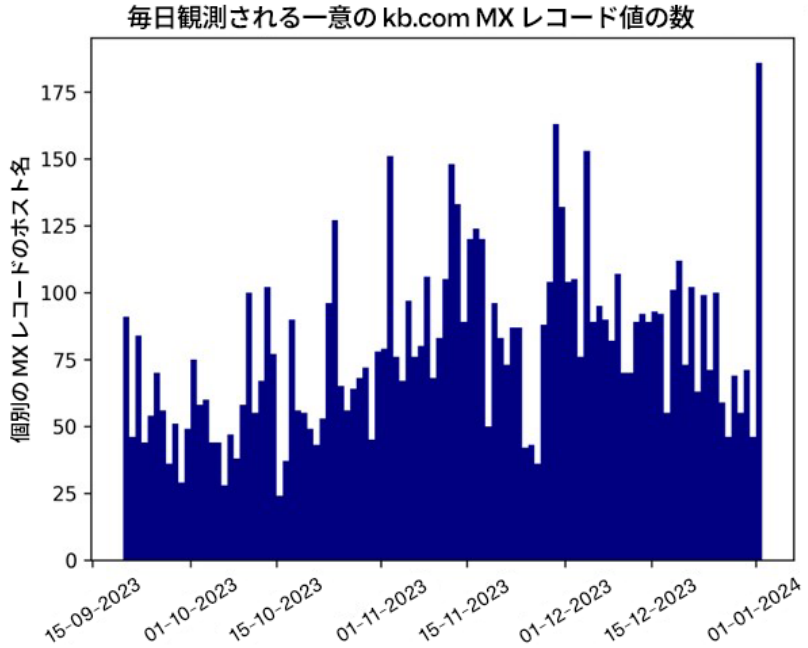

図5。グローバルpDNSコレクション内のkb[.]comの一意のMXレコード値の毎日のカウント。これらはドメインゾーンファイルに存在しない偽のMXレコードです。

また、数年にわたるkb[.]comのMXレコードの回答履歴も分析しました（図6）。ランダムなホスト名を含むMXレコードは、2019年10月15日に初めて確認されました。Muddling Meerkatのターゲットドメインの最初のMX解決が最初に確認されたのは、2019年10月15日頃であることを、他のベンダーと独自に検証しました。これは、分析したすべてのターゲットドメインに当てはまります。全体的に、サードパーティのデータでは、2023年9月20日から2024年初頭にかけて、MX解決の数に不可解な増加が見られます。

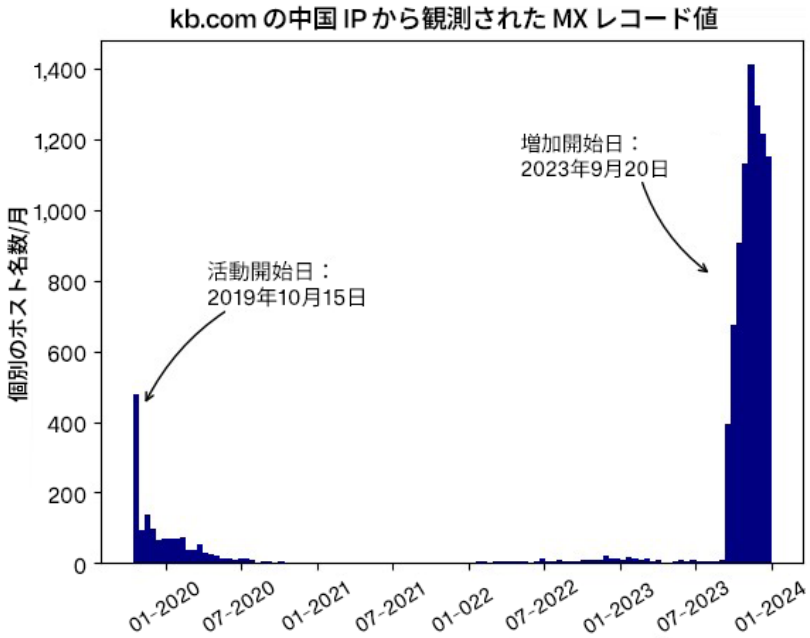

図 6。kb[.]com の一意の偽の MX レコード値の数。これは、時間の経過とともに毎月集計され、サードパーティの DNS データ収集で観測されています。これらの解決の応答 IP アドレスは、DNS サービスをホストしていないランダムな中国の IP アドレスであり、応答が Great Firewall から来ていることを示しています。これらはすべて、kb[.]com DNS ゾーンファイルに存在しない偽の MX レコードです。

通常の DNS 解決パスに沿った再帰リゾルバーまたは他のサーバーでは、これらの応答が見られる可能性は低いです。Infoblox と DomainTools Farsight の両方からの kb[.]com の MX レコードの全履歴を比較した結果、一意なレコードはわずかな数しか確認できませんでした。2024 年 1 月現在、kb[.]com は、リゾルバーからの MX レコードリクエストに応答しません。過去に、権限のあるサーバーは、次の値を含む回答を返していました：

- mail.kb[.]com、smtp1[.]com、smtp2[.]com、smtp3[.]com

kb[.]com の権威ネームサーバーは公式の DNS 解決プロセスを通じては MX クエリに応答しませんが、当社の再帰リゾルバーはこれらのレコードの要求を受け取ります。通常、これらの要求を受け取るということは、当社の顧客ネットワーク内のユーザーが kb[.]com のユーザーに電子メールを送信する必要があることを意味します。しかし、kb[.]com はメールを提供しません。パッシブ DNS ログには奇妙なことが多数含まれており、古いアプリケーションやウェブサイトによってクエリがトリガーされることがあります。ただし、この場合、クエリは数か月にわたってちょうど 1 か月間隔で発生しているところが興味をそそります。次のセクションの他のデータからわかるように、この動作は、おそらく Muddling Meerkat がオープンリゾルバーを探して当社の顧客ネットワークを調査し、時折いくつかが見つかったことによって引き起こされた可能性が高いです。

私は、Muddling Meerkat のターゲットドメインなどについて、GFW からの偽の MX 応答を手動でトリガーすることができませんでした。おそらく、レコードは GC によって、または特定の Muddling Meerkat 運用コンテキストで生成されたものと思われます。例えば、応答は、アクターを識別する IP パケット内の署名によってトリガーされた可能性があります。ExploderBot IP パケットには、必要に応じてソースのチェックとして使用できる複数のアーティファクトが含まれていたことがわかっています。これにより、他の研究者が CNAME インジェクションを見た理由が説明できるかもしれませんが、これは稀です。残念ながら、これはすべて GFW/GC による異常な動作の可能な説明と過去の経験に基づいた推測にすぎません。応答自体が偽の IP パケットである可能性もありますが、「オッカムの剃刀の原則」に従えば、GFW の一種、特に GC の可能性が高いと言えます。可能性は多くありますが、信じられるものは少ないのです。

ランダムサブドメインの MX レコード

Muddling Meerkat 動作の 2 つ目の識別要素も MX レコードクエリに関係していますが、ベースドメイン自体ではなく、ターゲットドメインのランダムなサブドメインに対するものです。このイベントでは、通常の状況では、クエリは、ユーザーがベースドメインではなくサブドメインに電子メールを送信したい場合にトリガーされます。このシナリオは通常の DNS でも発生しますが、特に一般的ではありません。Muddling Meerkat ターゲットドメインのほとんどには機能するメールサーバーがないため、さらに異常な状況が生じます。実際、kb[.]com のランダムなサブドメインの MX レコードに対するクエリが、この調査全体のきっかけとなりました。

私たちの再帰リゾルバーでは、ランダムなホスト名を伴う少数のリクエストが、1 ～ 3 日間にわたって発生するという現象が観測されました。これらのリクエストには MX レコード以外のクエリタイプも含まれますが、通常のネットワーク運用における MX レコードは特殊な性質を持っているため、このタイプに関する調査結果のみを報告します。MX クエリの形式は次のとおりです：

```
<random>.target_domain
```

<random> とは可変長の英数字文字列で、通常は 3 文字から 6 文字の長さです。

この調査は kb[.]com から始まりましたが、2023 年 9 月 1 日以降、当社の顧客ネットワークでは約 10 の Muddling Meerkat ターゲットドメインが観測されています。図 7 と図 8 は、9 月 1 日から 12 月 31 日までの間に当社の再帰リゾルバーで観測された kb[.]com と 4u[.]com の MX クエリの量と、特定の日にクエリされたサンプル FQDN を示しています。この 4 か月間、サブドメインは重複していません。当社のパートナーである DomainTools Farsight やその他の非公開ベンダーも、ランダムなサブドメインは異なるものの、同じ傾向を確認しています。

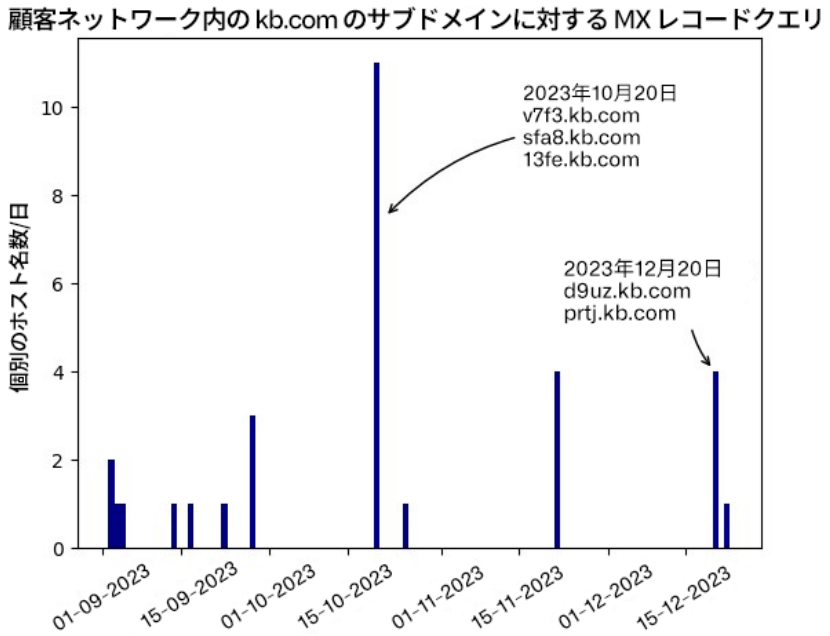

図 7。4 か月間に Infoblox の再帰リゾルバーで確認された kb[.]com の MX レコードクエリを持つ個別の FQDN の数

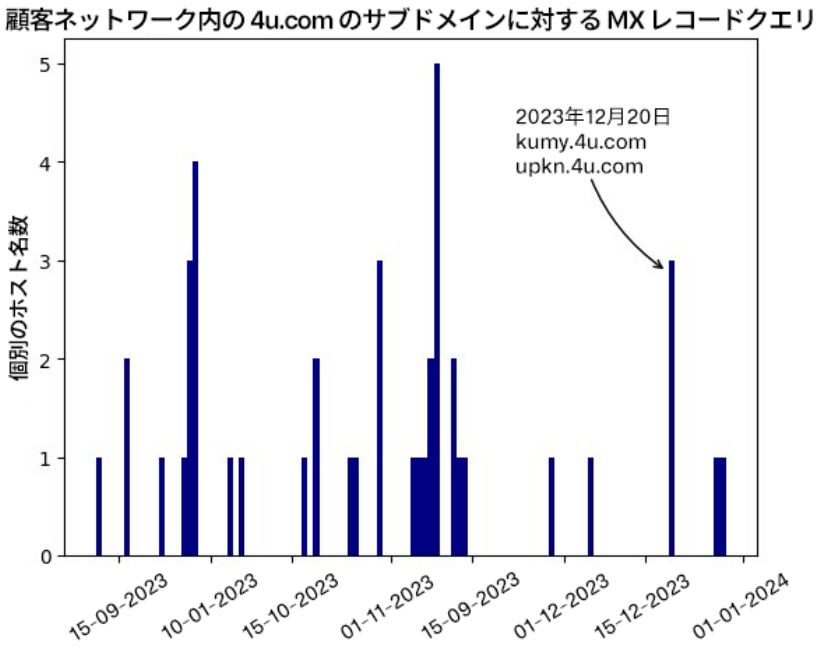

図 8。4 か月間に Infoblox の再帰リゾルバーで確認された 4u[.]com の MX レコードクエリを持つ個別の FQDN の数

図 7 と 8 は、1 日から 3 日間動作し、ランダムなホスト名を使用する Muddling Meerkat クエリの非周期的な「ポップアップ」特性を示しています。この種のパターンは、一般的なスロードリップ DDoS 攻撃、特に ExploderBot によく見られます。しかし、文献で以前に報告されたものとこれらの攻撃との間には、いくつかの重要な違いがあります。最も注目すべきは、これらの攻撃の規模が、実際の DDoS 攻撃で予想される規模や、2014 年から 2017 年にかけてこの活動がピークに達したときの大規模攻撃で見られた規模よりもはるかに小さいことです。

2019 年に Digital Threats Research and Practice 誌に掲載された縦断的研究で、ExploderBot に関する最初の論文以来、私は Slow Drip DDoS の状況が大きく変化したと指摘しました。[16] 2018 年に 6 か月間にわたって実施されたこの調査では、いくつかのクエリタイプが観察されましたが、MX はその中に含まれていませんでした。この論文で説明されている主要なパターンは現在でも観察されており、長いホスト名を持つクエリのレベルは低く、文字分布には強い偏りがあります。Muddling Meerkat はこれらのトレンドと類似点はありません。

ランダムサブドメインの IPV4 レコード

ターゲットドメインのランダムなサブドメインの MX クエリに加えて、再帰リゾルバーは A レコード、つまり IPv4 アドレスのリクエストを受け取ります。もちろん、権限のあるネームサーバーにはそのようなサブドメインが設定されていないため、これらのクエリはリゾルバーからの回答を受け取りません。再帰リゾルバーからコレクションを得る他のベンダーも同様の見解を持っています。例えば、DomainTools Farsight のデータは、世界中の再帰リゾルバーのコレクションから取得されます。Infoblox と同様に、これらのベンダーは、A レコードクエリを含む、Muddling Meerkat ドメインのランダムサブドメインに対するクエリの定期的な急増を確認しています。図 9 は、2024 年 1 月の 1 か月間の傾向を示しています。

16 Reneé Burton. 2018. Unsupervised Learning Techniques for Malware Characterization: Understanding Certain DNS-based DDoS Attacks. Digit. Threat. Res. Pract. 37, 4, Article 111 (August 2018), 27 pages. https://dl.acm.org/doi/10.1145/3377869

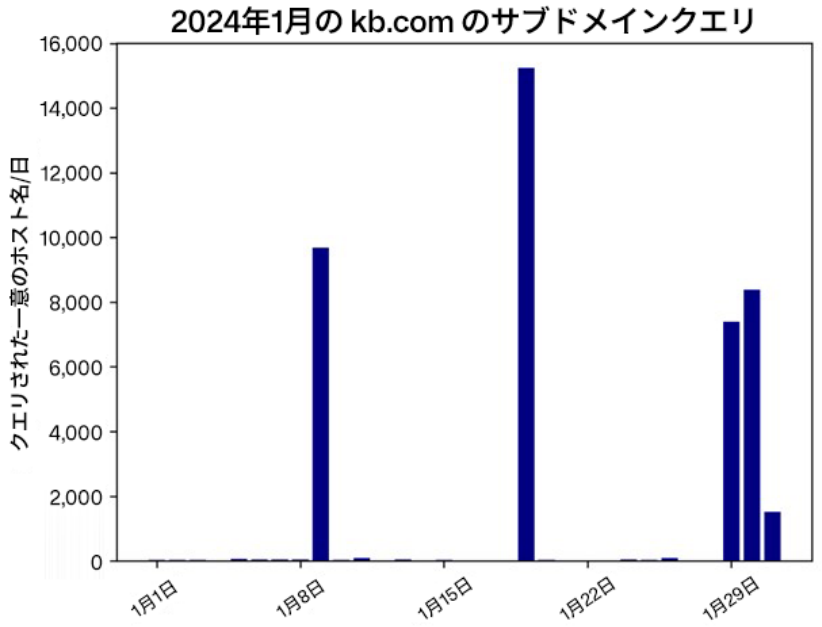

図 9。2024 年 1 月に Farsight pDNS で観測された kb[.]com の一意なホスト名クエリ。

パケット収集、ハニーポット、インターネットテレスコープなど、DNS を可視化する他の種類の収集もあります。ネットワーク内のこれらのクエリのソースはオープンリゾルバーであり、Muddling Meerkat はオープンリゾルバーを求めて幅広い IPv4 スペースを調査している可能性が高いという理論に取り組み、他のベンダーに、応答にリソースレコードを含むパケットを見つけるのを手伝ってもらいました。MX レコードの応答が見つかったのと同様に、A レコードの応答も見つかりました。

Muddling Meerkat ドメインの A レコードのクエリに応答した唯一の IP アドレスは、中国の IP スペースにありました。これらの IP アドレスはポート 53 で開かれていませんでした。これは、DNS リゾルバーではなかったことを示します。つまり、これらの回答は権威サーバーからではなく、GFW から送信されたものです。

GFW は、完全にランダムではない解決 IP アドレスを使用して DNS クエリへの回答を挿入することが知られています。2021 年 8 月に第 30 回 Usenix Security Symposium のために発表された 9 か月にわたる縦断的調査で、研究者は、偽造された IP アドレスが特定のドメイングループで繰り返し表示されることが多いことを発見しました。[17]

kb[.]com のサブドメインの解決 IP アドレスを使用して、偽造された解決 IP アドレスの発生をクエリのタイムラインにマッピングしました。すべてのケースで、解決 IP アドレスは、短いランダムなサブドメインに対して、1 日から 3 日間続く明確な時間ウィンドウで繰り返し見られます。図 10 と 11 は、この動作の 2 つの例を示しています。2 つの IP アドレスは実際には kb[.]com とは関係ありません。これらは GFW からの偽の回答です。両方の IP アドレスには重複する日に見られます。各図は、2022 年に kb[.]com サブドメインがその IP アドレスに解決された全体を示しています。Infoblox および Farsight リゾルバーデータと同様に、ホスト名またはサブドメインは繰り返されません。

17 How Great is the Great Firewall? Measuring China’s DNS Censorship. Nguyen Phong Hoang, et al., 30th USENIX Security Symposium (USENIX Security 21), https://www.usenix.org/system/files/sec21-hoang.pdf（最終アクセス日 2024 年 1 月 9 日）

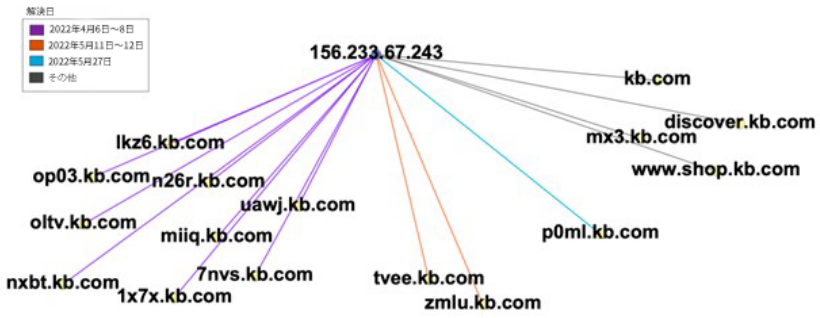

図 10。2022 年に GFW が kb[.]com ドメイン内で IP アドレス 156[.]233[.]67[.]243 に解決したホスト名。この IP アドレスは kb[.]com とは関係がなく、回答は GFW によって偽造されたものです。

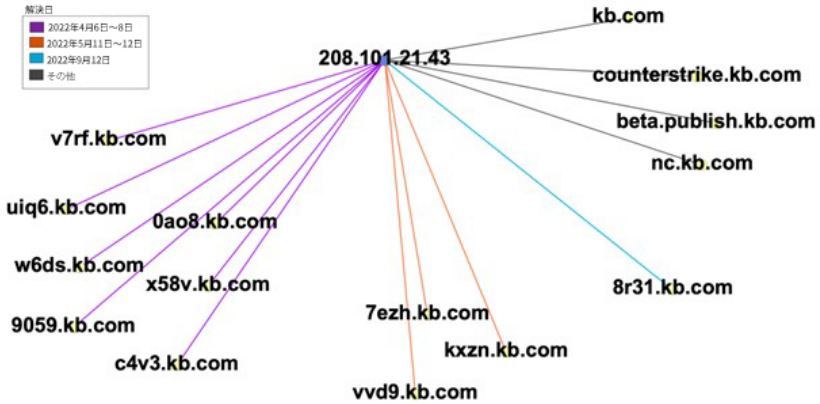

図 11。2022 年における kb[.]com ドメイン内の GFW による IP アドレス 208[.]101[.]21[.]43 へのホスト名解決。この IP アドレスは kb[.]com とは関係がなく、回答は GFW によって偽造されたものです。

これらの結果は、Muddling Meerkat が、場所や開いているポートに関係なく、多数の宛先 IP アドレスへの DNS クエリを含む操作を実行していること、および GFW が特定の日に、時間の経過とともに使用される一連の IP アドレスを使用してこれらのドメインへの応答を挿入していることを示しています。この同じアクティビティと種類の応答は、2024 年 1 月も継続しています。これらの数値は kb[.]com の解決を示していますが、既知の Muddling Meerkat ターゲットドメインすべてで同じパターンを確認しました。

ここからが面白いところです。GFW は通常、kb[.]com やサブドメインの応答を挿入しません。GFW は kb[.]com のランダムなサブドメイン要求に偽の応答を挿入しているわけではなく、Muddling Meerkat によって作成されたもののみを挿入しています。前述したように、GFW は人気のあるドメインや、中国の利益に何らかの形で反すると判断したドメインに応答を挿入します。前述の Usenix 論文はこの事実を検証しています。図 12 は、google[.] com への偽の応答を取得するために以前に使用した IP アドレス 111[.]193[.]204[.]201 からの nxbt.kb[.] com への A レコードクエリに対する 2024 年 1 月 13 日の応答を示しています。

```
; <<>> DiG diggui.com <<>> @111.193.204.201 nxbt.kb.com A
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

図 12. 111[.]193[.]204[.]204 からの nxbt[.]kb[.]com への A レコード要求に対する応答。この IP アドレスは中国の IP アドレス空間にあり、ポート 53 では開いていません。この応答は、このタイプのクエリに対して予想されるものであり、GFW の既知の動作と一致しています。画像提供：diggui.com。

MUDDLING MEERKAT のターゲットドメイン

Muddling Meerkat のターゲットドメインの選択は、DNS の洗練度を示しています。Muddling Meerkat のオペレーターは、通常の GFW 検閲では起こらない GFW からの選択的な反応を誘発します。そのために、彼らは自分が管理していないターゲットドメインを選択しており、セキュリティアプライアンスがブロックする可能性は非常に低いです。さらに、一般的に監視されていないクエリタイプを使用し、通常の DNS トラフィックと混ざり合う大量のクエリを作成します。Infoblox のリゾルバーでは、クエリタイプ A（IPv4）、CNAME、MX、AAAA（IPv6）のランダムなホスト名を確認しています。

私たちが観測したランダムなサブドメインクエリは、登録されてから 20 年以上経過し、ラベルが短く、TLD が .com や .org であるドメインに対するものでした。ターゲットドメインラベルはほとんどが 2 文字または 3 文字ですが、4 文字の例もいくつか見られました。（例:boxi[.]com）。ほとんどの場合、ドメインは時間の経過とともに所有者が変わりますが、元の作成日は WHOIS に引き続き表示されます。例としては、kb[.]com、4u[.]com、id[.]com、od[.]com、ntl[.]com、nef[.]com などがあります。これらのドメインはすべて、2023 年 12 月から 2024 年 1 月にかけて Infoblox リゾルバーの Muddling Meerkat トラフィックで観測されました。

私は複数のソースで約 20 件のターゲットドメインを確認しましたが、実際はおそらくこれよりも多いでしょう。ここで紹介し、後ほど「中国の IP アドレスの役割」というセクションで詳しく説明するいくつかの理由により、ターゲットドメインを分離することは困難です。まず、基本的な年齢と長さの基準を満たすすべてのドメインがターゲットになっているわけではないようです。例えば、rr[.]com、ibm[.]com、aol[.]com は基本的な要件を満たしていますが、Muddling Meerkat 操作で使用されているという証拠は見つかりませんでした（はい、aol[.]com は依然として DNS トラフィックに存在します）。当社の再帰リゾルバーでのクエリで見つかったドメインのほとんどは、使用されていないか（例 :4u[.]com）、顧客の間で特に人気がありません。kb[.]com や od[.]com など、多くはオフショアの中国語ギャンブルサイトで使用されています。National Instruments が所有する ni[.]com など、いくつかは定評があり、頻繁に使用されるドメインです。

定評のある TLD で、長い歴史を持つ短いドメインを使うという選択は、セキュリティアプライアンスにブロックされる可能性を減らすためだけではありません。これらの特徴を持つドメインは、

- 組織によって DNS 検索ドメインや Active Directory ドメインとして使用されることが多く、
- マルウェアでは調査員を惑わすためのフェイクとしても利用されます。

その結果、これらのターゲットドメインへの疑わしいクエリに気付いたセキュリティオペレーションセンター（SOC）のアナリストは、クエリに関連する可能性のある Malware の潜在的なソースが多数存在することになり、対応に困惑することになります。例えば、ベンダー VirusTotal が保存したサンプルでは、ドメイン kb[.]com には、このドメインを参照するファイルが 30 件以上、このドメインと通信するファイルが 7 件あります。[18] ドメイン od[.]com には 130 件を超える参照ファイルが表示されています。[19] これらの多くは古い Malware サンプルであり、ノイズを増加させます。

一方、私のような研究者は、アクティビティの全体像を理解しようとするため、関連のない DNS クエリをフィルタリングして、真のターゲットドメインを分離する必要があります。このタイプのドメインは、組織がドメインを管理していなくても、Active Directory でよく使用されます（これは危険な行為です！）。さらに、アプリケーション、ウェブサイト、および人間が DNS で異常なクエリを引き起こします。Muddling Meerkat が使用するクエリタイプの範囲の中で、MX は最も分析が簡単です。

18 https://www.virustotal.com/gui/domain/kb.com/relations

19 https://www.virustotal.com/gui/domain/od.com/relations

参考までに、2023 年 12 月 1 日から始まる 6 週間の間に発生した Infoblox リカーシブリゾルバーでの MX 解決を調査しました。メールサーバーのドメインについて考えると、それほど多くの多様性があるとは思えません。しかし、この期待は認知的バイアスだったのです。Muddling Meerkat に似た以下の条件を持つ SLD の数を数えてみました：

- .com、.org、TLD で
- NXDOMAIN 応答の結果が
- 10 を超える異なるホスト名を持つもの

1,100 件を超えるドメインが基準を満たしました。つまり、多くのドメインに異常な MX クエリがあるということです。これら 1,100 件のうち、ドメインラベルが 4 文字未満のものだけが含まれるようにセットを絞りました。その結果、調査期間中に 55 件の候補と 22,000 件を超える固有のクエリが生成されました。この候補セットから、他のさまざまな機能を使用してターゲットドメインを確認するための追加分析を実施しました。

オープンリゾルバーの役割

オープンリゾルバーは、任意のクライアントからのクエリに応答する IP アドレス上のデバイスですが、一般の人のために再帰リゾルバーとして意図的に設定されているわけではありません。対照的に、DNS のパブリックリゾルバーは、あらゆるクライアントからのクエリに答えるように設計された再帰的リゾルバーで、通常は Google、Cloudflare、Yandex などの大企業によって運営されています。一部の研究者は、オープンリゾルバーの定義にパブリックリゾルバーを含めていますが、私は含めていません。オープンリゾルバは、DDoS 攻撃の悪用ポイントとしてよく知られています。これらは、リフレクション攻撃の被害者に対する攻撃を増幅するために使用できます。リフレクション攻撃では、被害者の IP アドレスを含むなりすましのソースを持つリゾルバーに対して DNS クエリが実行されます。[20] また、被害者が所有する権威あるネームサーバーにクエリを配信する Slow Drip 攻撃や、中間インフラストラクチャに対するさまざまな攻撃にも使用されます。[21]

ここでは、オープンリゾルバーを説明するために、DNS リゾルバーではなく IP アドレスという用語を使用しています。これは、オープンリゾルバーが非常に複雑だからです。例えば、オープンリゾルバー IP アドレスの前にファイアウォールなどのインターネットアプライアンスがあり、クエリを傍受して、GFW と同様に応答を偽造し、元の宛先 IP アドレスが DNS クエリに応答したように見せかける場合があります。返される応答は正しい場合もあれば、正しくない場合もあります。この動作は、インターネットサービスプロバイダー（ISP）による DNS クエリの傍受に関する研究者が説明した動作に似ています。[22]

オープンリゾルバーは DDoS 攻撃の一因となるだけでなく、その分析を妨げます。パブリックリゾルバーが持つような幅の DNS キャッシュがないため、ルートサーバーと TLD サーバーへのトラフィックが増え、完全な解決を余儀なくされることがよくあります。オープンリゾルバーのトラフィックを分析した私の経験では、多くの人が DNS に他の設定ミスがあり、通常は不必要な追加のトラフィックを生み出しています。例えば、ルートヒントをキャッシュせず、ルートサーバーの IP アドレスを継続的にクエリすることがあります。偽造された応答の可能性と組み合わせると、オープンリゾルバーは多くのノイズを生み出し、研究者にとって誤解を招くものになります。

---

20 A Matter of Degree: Characterizing the Amplification Power of Open DNS Resolvers, Yazdani, et al. Nature Switzerland AG 2022 O. Hohlfeld et al. (Eds.): PAM 2022, LNCS 13210, pp. 293–318, 2022. https://doi.org/10.1007/978-3-030-98785-5_13. https://annasperotto.org/publication/papers/2022/yazdani-pam-2022.pdf（最終アクセス日 2024 年 1 月 14 日）

21 NRDelegation Attack: Complexity DDoS Attack on DNS Recursive Resolvers, Yehuda Afek, et al., 32nd Usenix Security Symposium, 2023 https://www.usenix.org/conference/usenixsecurity23/presentation/afek（最終アクセス日 2024 年 1 月 14 日）

22 Who is Answering My Queries：Understanding and Characterizing Interception of the DNS Resolution Path, Baujun Lui, et al., 27th Usenix Conference, 2018 https://www.usenix.org/conference/usenixsecurity18/presentation/liu-baojun（最終アクセス：2024 年 1 月 14 日）

私が初めてオープンリゾルバーに出会ったのは、ExploderBot DDoS 攻撃の研究中でした。これらの攻撃では、標的ドメインのランダムなサブドメインに対する DNS クエリを含む IP パケットが、さまざまな場所のバックボーン付近のインターネット上に投下されました。送信元 IP アドレスと宛先 IP アドレスの両方が偽造され、長期的に合わせると IPv4 アドレス空間の大部分を占めていました。私たちの調査では、GFW からの偽造応答やオープンリゾルバーなど、前述のすべての問題に遭遇しました。ExploderBot は通常、数日間に渡ってこのような攻撃を行いましたが、周期性はありませんでした。2016 年以前は、月に何度も活動がありましたが、その後は減速し、非常に不規則になりました。表向きは権威ネームサーバーへの DDoS 攻撃ですが、ExploderBot がもたらした最大の被害は、再帰リゾルバーやロードバランサーを含む ISP のインフラでした。オープンリゾルバーがなければ、ExploderBot 攻撃は目立たなかったでしょうが、数年前から、アクター名には付けられませんでしたが、その活動はブログやメディアの報道で取り上げられました。ExploderBot は非アクティブであると考えられています。Infoblox で最後に確認されたアクティビティは 2018 年 5 月 18 日です。

オープンリゾルバーは、Muddling Meerkat 操作でも重要な役割を果たします。証拠によると、クエリは中国の IP スペースの幅広い IP アドレスに送信され、その多くはオープンリゾルバーです。DNS クエリの宛先 IP アドレスは時間の経過とともに変化する可能性が高く、Infoblox のような再帰的リゾルバーで「ポップアップ」シグネチャが作成されます。言い換えれば、Muddling Meerkat は、Infoblox クラウドリゾルバーで観察されるよりも頻繁にインターネットを混乱させているのではないかと、私は考えます。代わりに、私は特定の期間、数日間にわたって、私たちの顧客の外部 IP アドレスが Muddling Meerkat の宛先に含まれているのではないかと疑っています。（これは私の推測であり、活動の全容を把握できるデータ可視性はありません。）お客様の中には、知らず知らずのうちにネットワークにオープンリゾルバーを置いて、クエリを受け取り、解決のために当社のリゾルバーに転送している方もいらっしゃいます。操作のテンポに関係なく、Muddling Meerkat クエリは、お客様のデバイスがそれらを転送したときにのみリゾルバーに表示されます。

Muddling Meerkat は多くのオープンリゾルバを悪用します。データセンター内に設置されたサーバーもあれば、家庭用ルーターもあります。例えば、Shodan によって MikroTik ルーターとしてフィンガープリントされた IP アドレスが多数確認されました。[23]2024 年 1 月、これらの IP アドレスには、表 1 のサンプルオープンリゾルバーからのクエリが含まれていました。

クエリア IP アドレス	クエリ名
23[.]173[.]112[.]115	92ac[.]kb[.]com、mi2w[.]kb[.]com、3k04[.]kb[.]com
103[.]47[.]134[.]195	zve3[.]kb[.]com、rjlf[.]kb[.]com、mayf[.]kb[.]com
38[.]54[.]105[.]163	q0ce[.]kb[.]com、h5ow[.]kb[.]com、4e5r[.]kb[.]com

表 1。2024 年 1 月に観測されたクエリア IP アドレスとクエリの例。2024 年 1 月 31 日現在、これらの IP アドレスはすべてオープンリゾルバーをホストしていました。

なりすましのクエリアはありません

ExploderBot の経験から、私は Muddling Meerkat が偽装したクエリ元 IP アドレスと広範囲の受信者 IP アドレスを使用してインターネットに DNS クエリを挿入していると考える傾向がありました。しかし、私たちが発見した証拠は、その逆を示していました。特定の中国の IP アドレスが、不釣り合いな数の DNS クエリのソースとなっていたのです。データ（例については表 2 を参照）によると、Muddling Meerkat は専用サーバーを使用している可能性が高いように見えました。

23 Shodan.io は、IP アドレスによるサーバー属性の公開検索エンジンです。

反証があるにもかかわらず、私たちは偽装クエリ仮説を検証したいと考えました。そのための最良の方法は、**ネットワークテレスコープと呼ばれるものを使用することでした。**[24] これは、トラフィックが存在しない未使用の IP アドレスを利用し、そこにルーティングされるパケットを収集します。ネットワークテレスコープは、なりすましの IP アドレスを利用する大規模なイベントをキャプチャするのに役立ちます。Merit Network などの多数のテレスコープオペレーターは、約 1,100 万の IP アドレスへのトラフィックを観測できます。これらの IP アドレスは実際には使用されていないにもかかわらず、さまざまなプロトコルを含む膨大な量のトラフィックを受け取っています。

偽装された DNS クエリのコンテキストでは、一連のイベントは次のようになります：

- 攻撃者は、IP アドレス A から IP アドレス B 宛てに送信された DNS クエリを含む IP パケットを挿入します。
- IP アドレス B が DNS リゾルバ、または GFW のような目に見えないプロキシであると仮定すると、応答パケットが B から A に送信されます。
- この応答パケットは A で受信され、通信を開始しなかったアドレスへの反射であるため、テレスコープではバックスキャッターと呼ばれます。

テレスコープのオペレーターは、受信したバックスキャッターによってインターネットイベントを測定できます。これらのオペレーターは、インターネットトラフィックと特定の攻撃に対する独自のウィンドウを持っています。

Merit Network の研究者は、バックスキャッターデータで Muddling Meerkat の応答の証拠を見つけることができませんでした。Merit Network の研究者はその後、応用データ解析センター（CAIDA）にある別の大型テレスコープのオペレーターに連絡を取り、Muddling Meerkat が CAIDA テレスコープが監視している範囲のクエリア IP アドレスを偽装していないかどうかを確認しました。[25] AIDA には、このアクティビティに関連するバックスキャッターがキャプチャされていませんでした。彼らの結果を、中国の IP アドレスから発信された大規模な DNS クエリに関する以前の観察と組み合わせると、Muddling Meerkat がその活動においてクエリ元の IP アドレスを広範囲に偽装していないと確信できます。これは、Muddling Meerkat と ExploderBot の大きな違いです。

中国の IP アドレスの役割

Muddling Meerkat の活動には複雑さが伴い、GFW の影響もあるため、中国の IP アドレスを使用した特定のイベントが「本物」であるかどうかを判断するのは困難です。ここで言う「本物」とは、特定の IP アドレスが GFW の結果としてクエリに「回答」しているかどうかが不明確な場合があるということです。同様に、なりすましの IP アドレスとクエリの発信元の IP アドレスを区別するのは難しい場合があります。

この問題に対する私たちのアプローチは、全体的な統計から結論を導き出すことでした。前に説明したように、「ランダムサブドメインの IPv4 レコード」というタイトルのセクションで、その IP アドレスがポート 53 を開いていないことがわかっているのに、中国の IP アドレスが Muddling Meerkat のクエリに「回答」していることがわかりました。 このような例が多数あることから、「回答」は GFW の結果であり、「本物」の回答ではないと結論付けることができます。

クエリの行動を見ると、いくつかの IP アドレスが目立っています。これらの IP アドレスは、オープンリゾルバー IP よりもはるかに高い頻度で発生します。これらは、オープンリゾルバーをホストしていた IP アドレスへのものを含め、DNS の通常の解決範囲外だったクエリのソースです。これらのクエリア IP アドレスの中には、積極的なスキャンやその他の疑わしい行為が繰り返し報告されているものもあります。[26] 表 2 は、送信元 IP アドレスとクエリの例を示しています。

24 https://en.wikipedia.org/wiki/Network_telescope

25 https://www.caida.org/

26 https://www.abuseipdb.com/check/183.136.225.14?page=8

クエリア IP アドレス	クエリ名
183[.]136[.]225[.]45	ybzz[.]kb[.]com、xv9k[.]kb[.]com、0h5w[.]kb[.]com
183[.]136[.]225[.]14	y4fw[.]kb[.]com、mq5i[.]kb[.]com、h420[.]kb[.]com

表 2。2024 年 1 月に観測されたクエリア IP アドレスとクエリの例。これらの IP アドレスは、2024 年 1 月 31 日現在、オープンリゾルバーをホストしていませんでした。これらのクエリの一部は、既知のオープンリゾルバーに向けられたものです。

MUDDLING MEERKAT の活動を見つける

Muddling Meerkat は、いくつかの情報源から部分的に観察できます。私たちのような再帰的リゾルバーは、ランダムなサブドメインのクエリと、ターゲットドメインの MX レコードのクエリの両方を監視できます。グローバル DNS を介して解決されると、これらのクエリの大部分は NXDOMAIN 応答になります。ネットワーク内にオープンまたはパブリックリゾルバーがない場合、DNS ログに Muddling Meerka が表示されることはないと考えます。残念ながら、多くの DNS ログシステムは、成功した解決のみを記録しており、ネットワーク所有者は、この制限のために、アクティビティに気づかない可能性があります。

Muddling Meerkat のクエリは、それを観測できる人には断続的に現れる可能性があり、図 6 および図 7 の例と似た形で、ネットワークの規模に依存します。Infoblox では、世界中の顧客の DNS クエリを解決しているため、一般的な組織よりも多くの Muddling Meerkat トラフィックが発生します。当社のクラウド再帰的リゾルバーは、2023 年だけで 33 兆件を超えるクエリを処理しました。

DNS クエリログに加えて、研究者は他のさまざまなソースにも Muddling Meerkat の痕跡を見つけられるはずです：

- ルート、TLD、権威ネームサーバーにはすべて、2019 年 10 月、あるいはそれ以前にまで遡る Muddling Meerkat アクティビティの証拠が存在します。攻撃者はターゲットドメインを管理しておらず、広範な IP レンジに対してレコードをクエリしているため、オープンリゾルバーがクエリを転送し、解決チェーン内の各サーバーにリクエストが送られることになります。
- 再帰的リゾルバのキャッシュにも Muddling Meerkat の証拠が記録されます
- DNS ハニーポットの所有者は、Muddling Meerkat が IP アドレスをどの程度広範囲にクエリするかに応じて、クエリを受信する可能性があります。
- フローデータには、特に中国の IP 空間を監視している場合や、特にオープンリゾルバー IP アドレスから発生する、権威ネームサーバーへのポート 53 接続の異常な多様性を示している場合など、アクティビティの兆候が含まれている可能性があります。

このレポートの最後に記載されているドメインへのクエリは疑わしいと見なす必要があります。ただし、これらのドメインは Active Directory および DNS 検索ドメインとして幅広く使用されていることに注意してください。ターゲットドメインに加えて、特に短いランダムサブドメインの場合は、MX レコードのクエリが必要です。Muddling Meerkat ドメインのサブセットには他にも疑わしいクエリがありますが、このレポートには含まれていません。これらは、ネットワーク情報を権威サーバーに漏らすと思われる A レコードクエリです。しかし、このアクティビティを Muddling Meerkat と明確に結び付けることはできません。

属性と動機

Muddling Meerkat は、中国の国家主体の攻撃者であると考えられています。私たちは、Muddling Meerkat のターゲットドメインのポート 53 で開いていない中国の IP アドレスからの MX レコード応答を数年にわたって観察できているため、それらの応答が GFW の結果であると確信しています。同時に、GFW からの適切な MX 応答はこれまで報告されたことがなく、私を含む研究者は手動でこの動作を引き起こすことができませんでした。私たちが 4 年間にわたって観察してきたような選択的反応を誘発するには、Muddling Meerkat が何らかの形で GFW オペレーターと関連していると思われます。このような選択的な応答がどのようにトリガーされるのかはわかりませんが、ExploderBot のトラフィックで観測されたような IP パケットに含まれるシグネチャが、GFW からの異なる応答を知らせるために使用されている可能性があります。

これらの作戦の動機は不明です。私たちが持っているデータによると、操作は独立した「段階」で実行されており、一部にはターゲットドメインに対する MX クエリが含まれ、その他にはランダムなサブドメインに対するより広範なクエリセットが含まれます。GFW からの MX レコードを含む DNS イベントデータは、多くの場合、オープンリゾルバーで MX クエリが表示される日付とは別の日付に発生します。ドメイン名はステージ間で同じであり、クエリはドメイン名間で複数年にわたって一貫しているため、これらのステージは確かに関連しているはずですが、それらがどのように関連しているのか、またはなぜアクターがそのような段階的なアプローチを使用するのかについての結論は導き出されませんでした。

これまでに行われた調査を踏まえて、考えられる動機についていくつか考えてみましょう：

- これは DDoS 攻撃ですか？いいえ、少なくとも現在の形式のものではありません。観測されたクエリの量は、権威サーバーや中間リゾルバーに影響を与えるには少なすぎます。リフレクション攻撃が関与している兆候もありません。
- これはデータの流出ですか？その可能性は非常に低いです。アクターはオーソリティネームサーバーを管理しておらず、情報を運ぶ能力が最小限の短いサブドメインラベルを使用し、パケットを広範囲にブロードキャストし、返答経路を制御していないようです。
- これはオープンリゾルバースキャンですか？やはり、可能性は低いです。オープンリゾルバーを見つける方法は数多くありますが、どれも、これらのイベントで観察されるものよりも単純です。
- これはインターネットマッピングの試みですか？その可能性はあります。ただし、ネットワークをマッピングするのは非常に複雑な操作のように思えます。
- これは DDoS 攻撃の事前配置ですか？その可能性はあります。DDoS 攻撃を効果的に行うには、アクターは操作方法を大幅に変更する必要があります。
- これはある種のインターネット調査ですか？その可能性はあります。もしそうなら、それは非常に長期にわたる研究プログラムであり、私にははっきりとした目的はわかりません。
- これはソフトウェアのバグまたは他のアプリケーションの結果ですか？違います。この説明は、以前、私たちが実施した ExploderBot の研究に対する懐疑的な意見として提起されました。データには、これらが偶発的な DNS クエリであるという結論を裏付けるものは何もありません。Muddling Meerkat の活動は非常に意図的で、非常に巧妙です。

他の国家主体が GFW を装い、クエリと応答の両方を偽装している可能性はありますか？可能なことはたくさんありますが、すべてが現実的とは限りません。

結論と提言

私のように DNS をじっと見つめて長い時間を費やしていると、そこに何か正常なものがあるのだろうかと疑問に思うことがあります。この分野で何年も働いてきましたが、今でも新しい発見があり、アクターによる新しい行動を観察しています。多くの場合、無関係な他の要因の結果として新しいアクターが発見されます。このケースでは、中国の違法なギャンブルネットワークを調査した結果、異常な MX レコードを発見することになりました。いくつかの誤った手がかりを追いかけた後、外部の研究者とデータや分析を共有して協力することで、Muddling Meerkat の活動についてより明確なイメージを形成することができました。結局のところ、このレポートを書いているのは私ですが、分析と結論は、さまざまな関係者がそれぞれ異なる視点を持ち寄って共同作業を行い、これまで文書化されていなかった GFW の動作と、数年にわたる謎の DNS 操作を明らかにした結果です。

私たちの調査では、現代のインターネット通信の怠慢と複雑さから生じる潜在的なネットワークの脆弱性も浮き彫りになっています。特に、ネットワーク管理者には次のことをお勧めします：

- ネットワーク内のオープンリゾルバーを積極的に探し出して排除します。これらのデバイスを識別するのは難しい場合がありますが、Infoblox などの企業や Shadow Server Foundation などの組織が、役立つ重要な情報を提供しています。
- Active Directory または DNS 検索ドメインには、所有していないドメインを使用しないでください。ネットワークやユーザーアプリケーションに関する情報が、権限のあるネームサーバーや、制御できない他のアプライアンスに漏洩する可能性が非常に高いためです。この種の情報により、悪意のある人物が標的型攻撃の目的でネットワークを受動的に偵察できるようになります。
- DNS Detection and Response（DNSDR）をセキュリティスタックに組み込んでください。DNS に内在する脅威を効果的に処理できるのは DNS リゾルバーだけです。ほとんどのセキュリティ製品は、MX クエリと A レコードクエリの違いを認識しません。
- Muddling Meerkat の活動をコミュニティに報告してください。一つの視点から全体の範囲を観察することは不可能であるため、この脅威についての理解をクラウドソーシングすることが重要です。特に、Muddling Meerkat のドメインを追加で報告することは、他の人がオープンリゾルバーやネットワーク内のアクティビティを見つけるのに役立ちます。

最終的には、CISA が表明した中国に関する懸念と、世界規模でのサイバー攻撃のための事前配置という脅威について、私も同様に懸念を抱いています。私の専門的な経験では、中国の脅威アクターは、検閲、サイバー犯罪、DDoS 攻撃など、さまざまな目的のために DNS を管理、理解、活用することに非常に長けていると感じています。また、中国の脅威アクターには、この分野でもトップクラスの研究者がいます。Muddling Meerkat の本当の目的が何であれ、それを達成するための中国の才能と忍耐力を過小評価すべきではなありません。

活動の指標（ターゲットドメイン）

これらのドメインは、侵害の兆候ではなく、必ずしも悪意のあるものでもないことに注意してください。Muddling Meerkat が使用しているドメインの中には、パークされているものもあれば、ギャンブルサイトやその他の違法な可能性のあるコンテンツをホストしているものもあります。Muddling Meerkat のターゲットドメインの全範囲は、おそらくはるかに広範囲です。

これらのドメインは、ウェブサイトをホストしていないか、違法コンテンツをホストしているか、またはパークされています。影響なくブロックできる可能性があります：4u[.]com、kb[.]com、oao[.]com、od[.]com、boxi[.]com、zc[.]com、s8[.]com、f4[.]com、b6[.]com、p3z[.]com、ob[.]com、eg[.]com、kok[.]com、gogo[.]com、aoa[.]com 、gogo[.]com、zbo6[.]com、id[.]com、mv[.]com 、nef[.]com、ntl[.]com、tv[.]com 、7ee[.]com、gb[.]com、tunk[.]org、q29[.]org

これらのドメインはウェブサイトをホストしており、ブロックするとネットワークに悪影響を及ぼす可能性があります：ni[.]com、tt[.]com、pr[.]com、dec[.]com

攻撃を開始するために使用される IP アドレス :

- 183[.]136[.]225[.]45
- 183[.]136[.]225[.]14

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他社とは一線を画しています。Infoblox が選ばれる理由とは？それは、驚異的なまでの DNS スキルと、圧倒的な可視性です。DNS は解釈や追跡が非常に難しいことで有名ですが、当社の深い理解と独自のアクセスにより、インターネットの内部の仕組みを舞台裏で観察することができます。当社は、ただ防御するだけでなく、先を見越し、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 DNS Detection and Response 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とともに、誤検出率が驚くほど低くなります。

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: 20240216v1