infoblox

Threat Intel

混在するマルスパム：悪意のあるスパムにおけるなりすましドメインの利用

著者
Stelios Chatzistogias
Laura da Rocha
Renée Burton

目次

これは、最初は失敗した研究についての話のように見えるかもしれませんが、実際には、研究を続けた結果、全く別の発見に至った経緯についての話です。

2024 年 3 月、当社は、中国のグレートファイアウォールを介して不可解な DNS 操作を実行する「Muddling Meerkat」と呼ばれる攻撃者に関するブログレポートを公開しました。研究に多くの時間を費やしましたが、これらの複数年にわたるオペレーションの目的を解明することができませんでした。私たちは、その作業を社内に留めておくのではなく、その活動について知っていることを公開し、他の人々が自分の洞察を共有することで、業界全体として Muddling Meerkat の真の性質を理解できるようにしようと決めました。その試みは成功したようです。このブログは、ネットワークとセキュリティの専門家からアイデアを集めました。中には、Muddling Meerkat や、少なくとも DNS で見られる「ターゲットドメイン」に関する匿名のデータを提供してくれた方もいました。

追加研究提案の多くは、スパムのオペレーションを主題としていました。一部の組織は、所有するドメイン（通常は外部で使用されていない内部ドメイン）について、不正使用の通知を受け取っていました。こうした不正使用報告は、Google や Yahoo などの大手メールベンダーへの大規模なスパム配信の証拠であり、スパムの送信元 IP は圧倒的に中国に割り当てられていることを示していました。これは Muddling Meerkat の活動と一致しているように見えます。中国の IP 空間から発信された偽のメールサーバー（MX）レコードや、オープンリゾルバを通じて企業ネットワークに流入する同様の MX クエリが観測されました。

私たちと共有されたデータファイルの一つが、ある洞察をもたらしました。私たちは自社でいくつかの Muddling Meerkat の「ターゲット」ドメインを所有していたのです。つまり、DNS の観点からスパム関連の活動をよりよく理解するために、これらのドメインについて送られてきた不正使用報告や、権威 DNS ネームサーバーのログを利用することができました。しかし、当社は豊富なスパムデータを保有しており、これを時系列で分析することで、Muddling Meerkat の活動を示すキャンペーンを追跡できました。

本論文は、当社によるスパム追跡の成果です。正直なところ、Muddling Meerkat の理解に近づいたかどうか確信は持てておらず、一見すると失敗に思われるかもしれません。しかし、それらのスレッドを追跡することで、現代における悪意のあるスパム（マルスパム）キャンペーンにおけるドメイン偽装の使用について多くのことを学びました。現代の攻撃者がドメイン偽装をどのように利用しているかを示す、いくつかの興味深い「獲物」をご紹介します。これらはすべて、Muddling Meerkat の行動と一部共通しています。これらのキャンペーンを、当社が受信者から受け取った不正行為の報告、および当社の権威 DNS ログと関連付けることができました。さらに、当社は偽装されたドメインの一部を所有しているため、それらの一部をメールサーバーへのバウンスとして受信しました。これらの情報源を行き来することで、Muddling Meerkat のターゲットドメインの範囲についてさらに理解を深め、当初報告したドメインのセットは、約 20 から 650 以上に拡大しました。

最も驚くべきことは、スパムにおいてドメイン偽装がどれほど広範囲にわたっているかということです。スパム全般、特になりすましからユーザーを保護するために設計されたメカニズムはいくつかありますが、なりすましドメインは依然として広く悪用されていることがわかりました。ほとんどのキャンペーンは中国の IP アドレスから送信されており、キャンペーンの種類の多様性は非常に注目に値します。セキュリティ対策が施されているにもかかわらず、なりすましドメインの使用は依然として経済的な利益をもたらします。この論文では、以下の内容について述べます。

- PDF 添付ファイルの QR コードを利用して中国国民から窃取する最近のキャンペーン
- 日本のユーザーを標的にした人気ブランドのなりすましによるログイン資格情報の窃盗
- ユーザーを騙して脅威アクターの暗号ウォレットにお金を払わせようとする、おそらくボットネットの残骸によって引き起こされる旧来の恐喝キャンペーン
- 悪意のある内容も動機もないように見える謎の金融キャンペーン

さらに、Muddling Meerkat を理解する試みにおいて、独自の権威 DNS サーバーログを使用したところ、代わりにこれらのスパムキャンペーンを検出した経緯について説明します。

スパムにおけるドメイン偽装

脅威アクターは、電子メールの送信者アドレスを偽装（なりすまし）することができます。これは、電子メールをより信頼できるものに見せかけるためです。何年も登録されているドメインを使用することで、送信者ドメインの年齢を確認して悪意のあるスパムを特定するセキュリティメカニズムを回避しやすくなります。一方で、攻撃者が amazon[.]com のような有名なドメインを偽装した場合、受信メールサーバーは、これらのドメインを使用したメールが偽装されたかどうかを判断するためのいくつかのメカニズムを持っています。スパマーが古く放置されたドメインを使用するのは、この検出リスクがあるためであり、これは Muddling Meerkat がその活動に好んで使用するドメインの種類と非常に似通っています。

メールサーバーが電子メールを受信すると、DNS でいくつかのチェックを行い、送信者の検証を試みます。次に、それらの結果をメールヘッダーと比較します。これらのチェックには、メールを受信した IP アドレスがそのドメインにメールを送信する権限があることを確認するなどのアクションが含まれています。これらのチェックの一部は、特定の DNS レコードに依存していますが、古い放置されたドメインには存在しないことが多く、ソフトフェイルが起こる可能性があります。

サーバーが標準的なチェックを実行し、該当する場合は追加のメールセキュリティアルゴリズムを適用した後、電子メールがスパムとしてマークされたり、隔離されたりする可能性があります。他のケースでは、ユーザーの受信箱に届くこともあります。マルスパムの攻撃者は、偽装メールが十分な数のスパムトラップを通過してユーザーに届き、報酬を得ることを期待しています。

権威 DNS サーバーとスパム

当社は、20 年近くもコンテンツを積極的にホストしていない、未使用のドメインを偶然にもいくつか所有しています。それらのドメインには、送信者ポリシーフレームワーク（SPF）レコードなど、送信者ドメインの信頼性をチェックするために通常使用されるものを含め、ほとんどの DNS レコードがありません。ドメインは短く、評判の良い TLD に属しています。これは、Muddling Meerkat やスパマーにとって理想的です。

皮肉なことに、当社の古いドメインのいくつかは、たとえば Tranco のトップ 100 万ドメインリストによく引用されています。これらのドメインの人気は、完全にスパムによるものだと思われます。このブログの主題から大きく外れずに言うと、当社の休眠ドメインの人気は、トップランキングを鵜呑みにしてはいけない理由の 1 つを明確に表しています。当社はドメインの人気と脅威の研究に多くの時間を費やしてきました。過去の論文をご覧ください。[1, 2]（脚注を読むには、この PDF をオンラインで表示してください。）

DNS は、当社ドメインの不正使用について、独自の視点を提供します。当社は、すべてのドメインのクエリを権威 DNS サーバーに記録しています。これらのログから、インターネットスキャンからスパムの配信まで、DNS アクティビティの幅広い範囲を垣間見ることができます。電子メールの場合、受信者のメールサーバーは、送信者ドメインの権威サーバーに対して、DNS TXT レコードを含む複数の DNS クエリを行います。当社は自社のログから、これらのメールサーバーが使用する DNS リゾルバーの IP アドレスを確認し、当社のドメインになりすましているスパムの地理的分布を把握することができます。

また、ドメインキー識別メール（DKIM）レコードを設定して、当社のドメインからスパムを受信したプロバイダーが不正使用報告をメールで当社まで送信できるようにしました。これらの不正使用報告には、スパム送信者の IP アドレスとタイムスタンプ情報が含まれています。これらの情報を DNS TXT レコードリクエストと組み合わせることで、スパム配信とどのように誤って関連付けられているかをかなり明確に把握できます。当社のメールサーバーはメールを送信せず、受信のみを行います。

当社は Muddling Meerkat による潜在的なスパム活動に関心があったため、潜在的なアクターのクエリを他のものから分離する必要がありました。DNS には多くのノイズがあります。当社のような研究機関の多くは、情報を収集し、履歴に合成フットプリントを作成するために DNS クエリを行います。すべてのドメインが休眠状態であるため、当社のサーバーは DNS クエリを受信しないはずですが、それでも毎日数千件、時には数万件のクエリを受信しています。図 1 は、4 つの異なる Muddling Meerkat ドメインに対して、権威サーバーで受信されたクエリ数の時間経過に伴う比較を示しています。上部のグラフはすべてのレコードタイプに対応しており、下部のグラフは MX クエリに対応しています。これらのタイムラインチャートは、メール関連の活動がドメインの全体的な DNS 活動と必ずしも相関していないことを示しています。

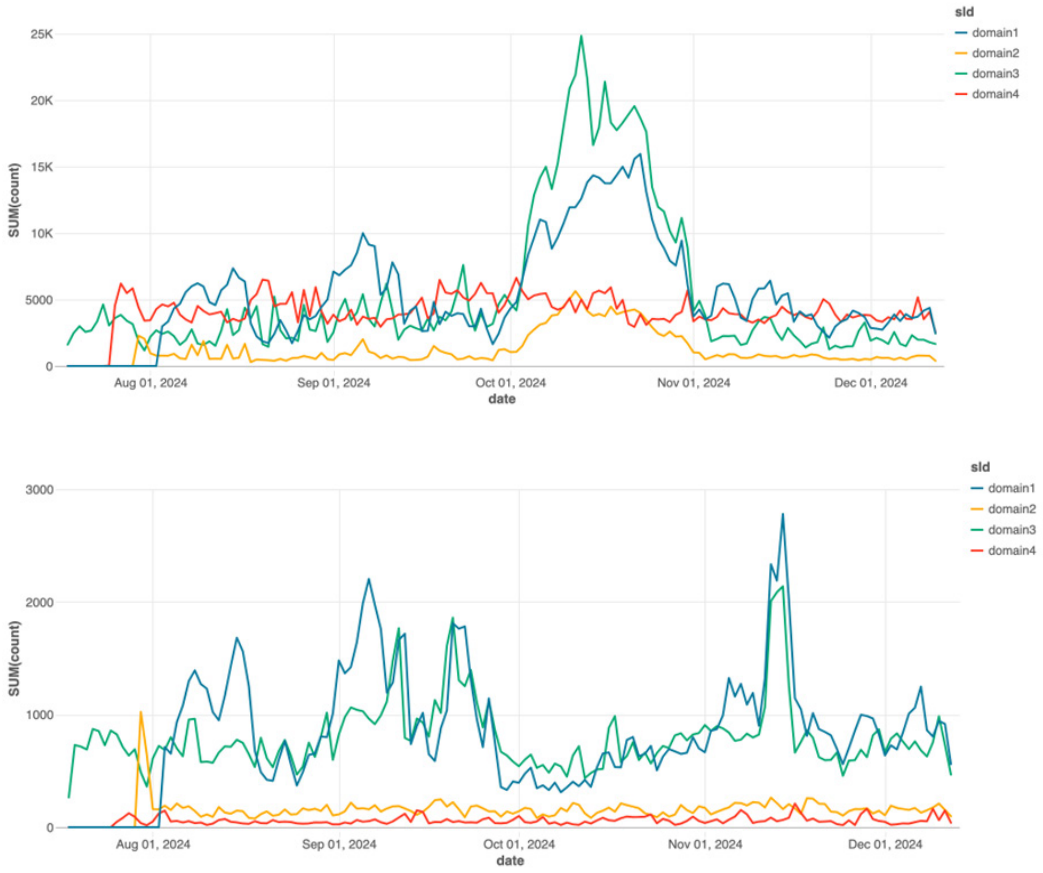

図 *1.* 上部のグラフ：権威サーバーで受信したすべての *DNS* レコードタイプ別クエリ数、下部のグラフ：*MX* レコードのクエリ数

当社の権威サーバーで受信するクエリの大半は Muddling Meerkat のパターンと一致しないため、過去の研究で作成した複数のフィンガープリントを用いて、攻撃者の潜在的な活動を特定しました。また、これらの調査結果を、メールで受け取った不正使用報告と比較しました。Muddling Meerkat の DNS クエリはさまざまなレコードタイプを使用しますが、調査の観点から最も珍しいのは、短いランダムなサブドメインに対する MX レコードクエリです。次の例では、ターゲットドメインが target.domain の場合、クエリは次のようになります。

```
<rand>.target.domain
```

ここでの「ターゲット」という用語は、以前の論文 [3] で説明したように曖昧なものです。攻撃者は、これらのドメインをドメイン所有者への攻撃の一環としてではなく、キャンペーンでの使用を目的としてターゲットにしています。攻撃者は、所有していないこれらのドメインを未知の目的で悪用しています。クエリの分析は、当社がサービスを提供している単一のドメインのサブドメインとしてのみ観測されたホスト名を持つクエリに限定し、傾向を調べました。一意に観測されたホスト名の長さはさまざまでしたが、3 文字のものが最も一般的でした(図 2 参照)。これは、他のドメイン所有者から受け取ったデータと一致していました。また、クエリが Google などの大手メールプロバイダーや Proofpoint などのメールセキュリティプロバイダーから送信されたことも確認しました。

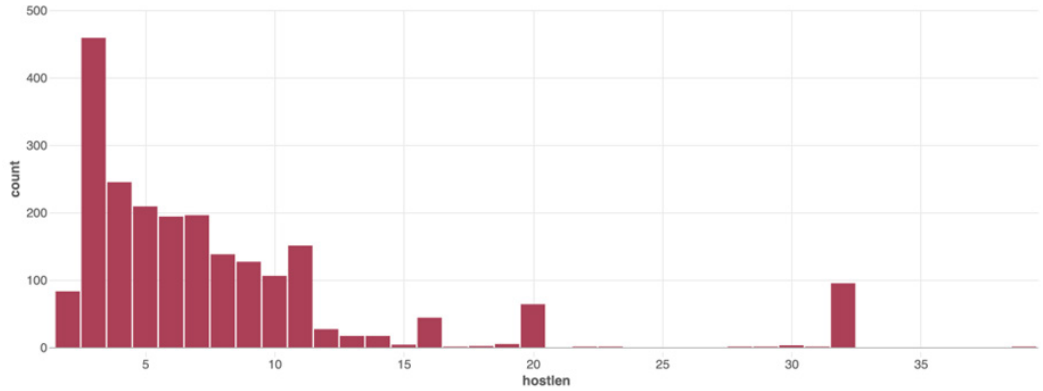

図 2. 当社権威 *DNS* サーバーにおいて一意に観測された *MX* クエリのホスト名長さ

当社のドメインが Muddling Meerkat に悪用され、マルスパムキャンペーンを実施する脅威アクターになりすまされていることが判明したため、スパムトラップでアクティブなキャンペーンを調査しました。

ケース #1：QR コードフィッシングキャンペーン

当社の古いドメインへのなりすましが観測されたフィッシングキャンペーンの中で最大のグループは、中華圏の住民を標的にしていました。これらのキャンペーンは少なくとも 2022 年後半から継続的に実行されており、フィッシングサイトに誘導する QR コードを含む添付ファイルを配布しています（図 3 参照）。DNS データ、不正使用レポート、および関連情報に基づくと、攻撃は中華圏から発生していると考えられます。このキャンペーンは、受信者に電子メールの添付ファイルを開かせ、WhatsApp を使用してその中の QR コードをスキャンさせる戦術を活用しています。この 2 段階の手法は、攻撃者が被害者をノート PC から暗号化されたチャットアプリに誘導し、多くの一般的なセキュリティ対策を回避するため、ユーザーの保護にさらなる課題をもたらします。また、脅威アクターは登録ドメイン生成アルゴリズム（RDGAs）を使用して、短期間のみアクティブになるランダムなドメインを作成します。

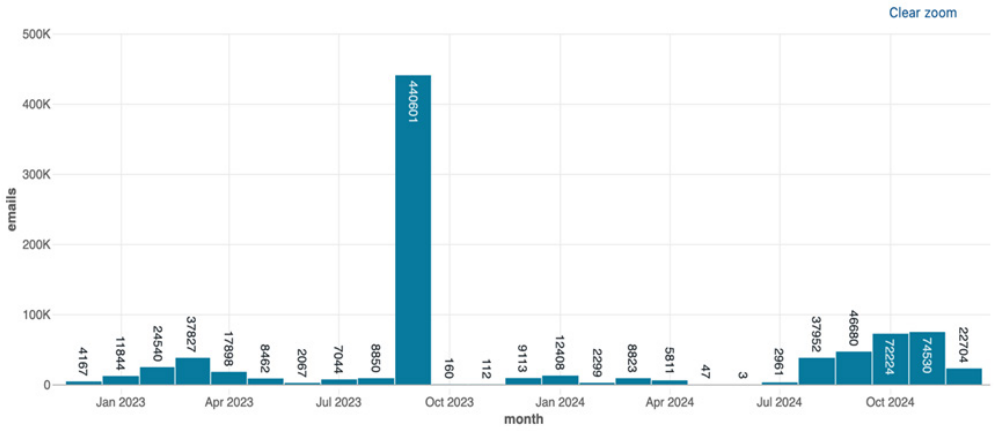

図 3. 中国の QR コードフィッシングメールの時間経過に伴う量

これらのマルスパムキャンペーンは、確認済みの Muddling Meerkat ターゲットドメインを多数含むなりすまし送信者ドメインを使用しており、その中には弊社が所有するドメインも含まれています。これらのキャンペーンのスパム分析と過去の DNS レコードの比較を通じて、既知の Muddling Meerkat ターゲットドメインの数は、2024 年 3 月時点の約 20 件から現在では 650 件以上に拡大しました。しかし、QR コードキャンペーンには、Muddling Meerkat が使用している可能性があるものの、DNS で確認できない多くのドメインも含まれています。

これらのキャンペーンでは、Muddling Meerkat DNS クエリで観察されたものと一致する構造を持つ送信者のメールアドレスが使用されています。送信者のユーザー名は、`<rand>@spoofed[.]domain` という形式の短いランダムな文字列でした。表 1 は、キャンペーンの送信者メールアドレスのサンプルを時系列で示しています。`jx[.]com` や `hm[.]com` などのドメインは、Muddling Meerkat のターゲットドメインとしてすでに認識されていました。

dm@**jx[.]com**	ino@**jjnywnd[.]com**
ab@**hm[.]com**	gwhy@**isathtooy[.]net**
zb@**iizlopn[.]com**	atmrp@**kym[.]net**
mu@**ibqg[.]net**	qivlzn@**kt[.]com**
xzu@**iejzhopjx[.]org**	atmrp@**kym[.]net**
iud@**irnvasa[.]net**	

表 *1*：*QR* コードキャンペーンにおける送信者アドレスのサンプル。送信者のメールアドレスには、<2 ～ 9 文字のランダムな文字列 >@< 偽装された *[.]* ドメイン > というパターンがある

メールには通常、2022 年 12 月またはそれ以前に開始された、北京語の税金関連の誘い文句が含まれています。これらは中国の IP 空間、主に 4134（Chinanet）と 56046（China Mobile）から発信されたものと思われます。図 4 は、いくつかの電子メールの件名とその英訳を示しています。

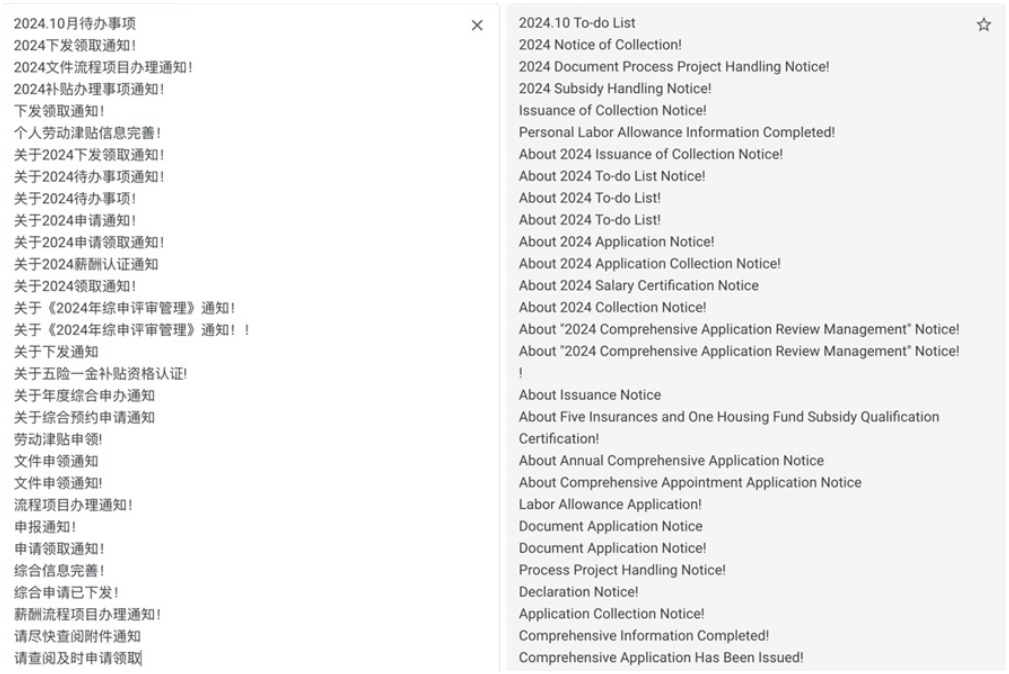

図 *4*：*QR* コードキャンペーンでのメール件名のサンプルとその翻訳

このマルスパムのもう一つの特徴は、QR コード文書のほとんどが 4 桁のパスワードで暗号化されていることです。このパスワードはメール本文のどこかに含まれていますが、一貫した方法ではありません。時には括弧で囲まれることもあり、他の記号で囲まれることもあります。図 5 は、電子メールにパスワードを含める方法を示す 2 つの例を示しています。

図 5. 4 桁のパスワードが異なるメールでどのように値や形式が異なるかを示す 2 つの例。赤と緑の枠線は、メール内でのパスワードの異なる表示方法を強調している。

添付ファイルには、ロゴが埋め込まれた QR コードと、受信者が Alipay/WeChat を使用してドキュメントをスキャンするための手順が含まれています。図 6 を参照してください。これらの電子メールは、補助金や金銭的利益を約束して脆弱な人々を狙うために、世界中でサイバー犯罪者が使用しているものと同様です。

図 6. 添付ファイルの内容と翻訳。ハイライトされた部分には、*Alipay/WeChat* を使用して *QR* コードをスキャンする指示が含まれている。

Twitter のユーザーが詐欺を報告しました。図 7 のツイート [4] によると、あるユーザーは QR コードをスキャンした後、カード番号と身分証明情報を入力するよう求められました。その後、金額と確認コードを入力するよう求められ、これはアカウントへの支払いだと思っていました。すぐに、カードから攻撃者に 590 ユーロが支払われたことを知らせるテキストメッセージが届きました。これは一通のスパムメールには相当な被害額です。

図 7. *QR* コードフィッシング詐欺に騙されたユーザーのツイート

この手口は、存続期間が非常に短く、特定地域に限定されていると思われる第 2 フェーズのフィッシング用ドメインに依存しています。これらのドメインは、約 1 日後には名前解決できなくなり、sbs、shop、life、bond、cn など、頻繁に悪用される TLD に属しています。これらのドメインは、aaaefiuibew[.]cn や 6ttox81[.]sbs などのランダムな文字列で構成されています。

この活動が Muddling Meerkat によるものかどうかは判断できません。一般的な PhaaS（Phishing as a Service）サービスである可能性が高いと思われます。キャンペーンは、Muddling Meerkat で見られる放置ドメインを使用しているものの、無効なドメインを含むランダム生成ドメインを広範囲に偽装しているようです。攻撃者はこの手法を使って、同じ送信者からのメールが繰り返されないようにするかもしれません。悪意のあるスパムからユーザーを保護するための努力にもかかわらず、これらのなりすましの中には、防御をすり抜け、被害を引き起こし続けるものもあります。

このアクティビティで確認された他の送信者ドメインは表 2 に示されています。

len2	len3	len4	len5
jt[.]net	iac[.]com	idhs[.]org	ivkpc[.]net
hc[.]com	izr[.]com	jxrn[.]org	jbdct[.]net
kk[.]net	koh[.]com	jirh[.]org	jfctl[.]org
jg[.]com	jwq[.]org	ismh[.]com	irnpc[.]net
kx[.]com	kcy[.]org	ikat[.]com	lahuf[.]net
len6	**len7**	**len8**	**len9**
jxjfwz[.]net	kbgpnek[.]org	jqmyuxk[.]com	hfababhqf[.]org
jxnsdf[.]net	ipcwfrn[.]com	jwruoytd[.]org	jfrcjfqjr[.]com
jwnlhr[.]org	iouwttz[.]com	ktfnmbxa[.]org	jkdduscaj[.]net
kindhy[.]net	jhrzbuk[.]org	jlsiwslr[.]org	jkjiwbpki[.]com
khznrl[.]com	hrggzxa[.]com	hrfliqoj[.]net	kwbjjlygw[.]net

表 2. *QR* コードフィッシングキャンペーンで見られる偽装ドメインのサンプル

QR コードキャンペーンが Muddling Meerkat 想定外のドメインを偽装していることに気づいた後、私たちは DNS とスパム収集に戻り、Muddling Meerkat の関与が疑われる別のキャンペーンを探しました。

ケース #2：日本におけるフィッシングキャンペーン

当社の権威 DNS サーバーでは、異常に多くのメール関連クエリに 3 文字のホスト名が含まれていることに気付きました。Muddling Meerkat によって作成された可能性のあるクエリを、スキャナーやその他のソースに起因するクエリから分離しようとした際、これらのクエリの量と一貫性は、調査に適した良い手段であるという感触がありました。その結果、同じクエリ構造を持つスパムの証跡を探しました。

当社は、日本のユーザーをターゲットにした一連のキャンペーンを発見しました。これらのメールには、日本全国の高速道路で使用されている電子料金収受システム (ETC)、三井住友銀行 (SMBC、日本最大の銀行の 1 つ)、Amazon、Mastercard などの人気ブランドが挙げられていました。これらのメールは、セキュリティ上の懸念やその他の問題を理由に、ユーザーにサービスへの認証を促します。メールに含まれるボタンをクリックすると、ユーザーはトラフィック分散システム (TDS) に誘導され、特定の条件が満たされると偽のログインページにリダイレクトされます。[5] この手法は不正広告でよく使用され、セキュリティ企業による検出を回避するために最終的なランディングページを隠蔽する際に使用されます。偽のログインページは、被害者が資格情報を入力すると、その資格情報を盗みます。図 8 は、これらのスパムメールの例を示しています。

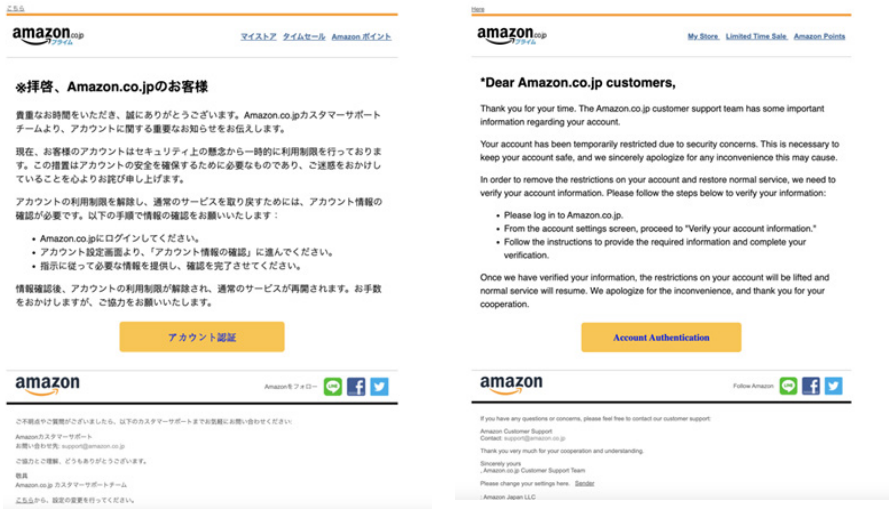

図 8. 偽の *Amazon* 警告を使って日本のユーザーをターゲットにした実際のスパムメールと、その機械翻訳

ユーザーが [アカウント認証] ボタンをクリックすると、以下のことが起こります。

- ubrjubf[.]com に誘導され、IP 43.128.150[.]42 で解決される
- その後、ユーザーは別のドメイン unpwple[.]com にリダイレクトされ、IP アドレス 43.133.182[.]243 で解決される
- ユーザーは偽の Amazon アカウントログインページに到達する。図 9 を参照

図 9. 偽の *Amazon* ログインページ。画像参照：*https://urlscan.io/result/5c9bbf63-883f-4eab-b4fc-45e2809a8ac2/*

Amazon をテーマにしたスパムのいくつかのバリエーションと、Mastercard や 三井住友カード会員向けサービス「Vpass」を使用したスパムなどが観察されています。[6] この攻撃者は専用のホスティングインフラストラクチャを使用し、同じドメインと IP アドレスを通じてキャンペーンをローテーションしています。[7] 観察された 2 つの専用 IP アドレスは、43.128.150[.]42 と 43.133.182[.]243 でした。表 3 は、キャンペーンで使用された RDGA ドメインの一覧を示しています。

43.128.150[.]**42**	**43.133.182**[.]**243**
eujsubf[.]com, eujsxikw[.]com,	anzcinf[.]xyz, anzconc[.]xyz,
ikhcok[.]com, insjibr[.]com,	infkokf[.]com, omfkiht[.]xyz,
insjkf[.]com, khcpw[.]com,	omfkybg[.]xyz, inybinf[.]com,
maczplw[.]com, maczunf[.]com,	unpwple[.]com, inybubf[.]com,
pknribt[.]com, pknrinf[.]com,	pplaaej[.]com, eccteukx[.]com,
pknrinr[.]com, pknrohv[.]com,	espoeubf[.]com, unpwmlw[.]com,
pknrybg[.]com, pknrynf[.]com,	pplaaeu[.]com, ecctenje[.]com,
ubrjpnf[.]com, ubrjubf[.]com,	unpwibr[.]com, ecctepje[.]com,
unpwinf[.]com, uwkxubs[.]com,	pplaaep[.]com, pplaaea[.]com,
wkxaubf[.]com, wkxaunf[.]com	espoeunf[.]com, espoekwl[.]com

表 *3.* 日本のユーザーをターゲットにしたキャンペーンで使用された専用 *IP* アドレス上の *RDGA* ドメインの例

前のセクションで説明されたキャンペーンと同様に、これらのキャンペーンの電子メールは、Infoblox Threat Intel が所有するドメインを含む、偽装された送信者ドメインを使用しています。また、3 文字のサブドメインを持つ当社の権威 DNS サーバーや、メールプロバイダーから受け取った不正行為報告で一般的に見られる形式にも一致しています。表 4 は、送信者のメールアドレスの例を示しています。

ak@fdd.**xpv**[.]**org**	iipnf@gvy.**zxdvrdbtb**[.]**com**
mh@thq.**cyxfyxrv**[.]**com**	zmrbcj@bce.**xnity**[.]**net**
mfhez@shp.**bzmb**[.]**com**	nxohlq@vzy.**dpyj**[.]**com**
gcini@vjw.**mosf**[.]**com**	

表 *4. 3* 文字のサブドメインを持つ、日本のフィッシングメールの送信者アドレスのサンプル。*3* 文字のホスト名は赤色で表示され、なりすましドメインは太字で表示している。

日本のユーザーを狙ったキャンペーンは、これだけではありませんでした。もう一つの大きなスパムは、人気のある暗号通貨ウォレットである MyEtherWallet を含み、類似ドメインを使用していました。スパムメッセージには、「(重要なお知らせ) MyEtherWallet ご利用確認のお願い」といった日本語のテキストが含まれることがあり、ユーザーにアカウントへのログインを求めます。図 10 は英語のメールの例を示しています。リンクは本物のウェブサイトのように見えますが、実際には脅威アクターによって作成された類似ドメインに誘導されます。

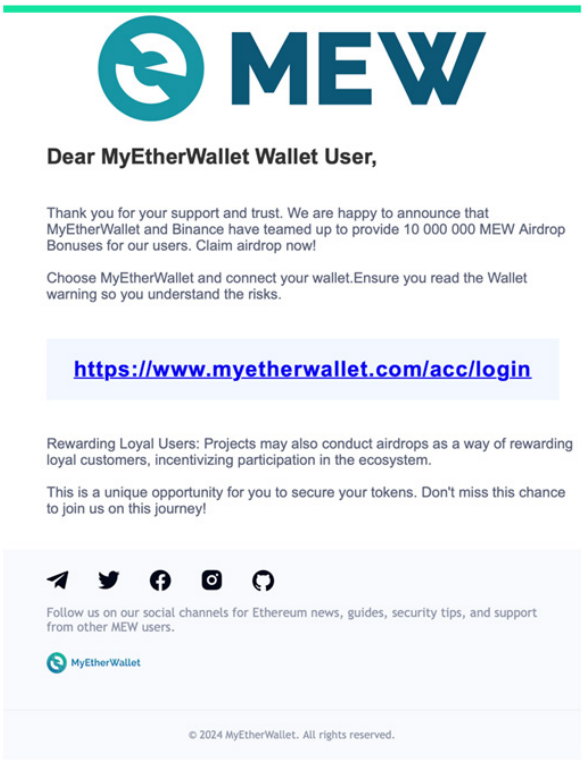

図 *10.* 日本のユーザーを標的としたスパムキャンペーンのサンプル。この特定のメールの件名は「*Binance Distribution of MyEtherWallet (MEW) Airdrop*（*Binance* 社が *Airdrop* で *MyEtherWallet* (*MEW*) を配布）」で、ユーザーを `myetherwallatak[.]org` に誘導。

類似ドメインは MyEtherWallet のウェブサイトのミラーコピーへと誘導し、ユーザーの認証情報を盗むために使用されました。これらのドメインは、com や org を含むいくつかの異なる TLD にあります。サンプルについては表 5 をご覧ください。

myetherwalletie[.]com	myetherwalletih[.]com	myetherwalletik[.]com
myetherwalletiv[.]com	myetherwalletjp[.]com	myetherwalletrt[.]com
myetherwallettv[.]com	myetherewallet[.]org	myetherswallet[.]org
myetherwallata[.]org		

表 5. 日本のユーザーの認証情報をフィッシングするために使用される類似ドメインのサンプル

QR コードフィッシングキャンペーンにおいて、いわゆる送信者アドレス、すなわち受信者に表示されるメールアドレスに、Muddling Meerkat のドメインが確認されました。しかし、この日本語のサンプルでは、ドメインはメッセージの「送信元 (received from)」部分に表示され、SMTP を介した技術的な配信に使用されます。当社は、Muddling Meerkat の活動で観察されたものと同じドメイン(類似のサブドメイン形式を含む）を使用する別の一連の悪意のあるスパムキャンペーンを発見しましたが、それが Muddling Meerkat によるものであるかどうかは確認できませんでした。表 6 では、なりすましドメインのサンプルを示しています。

len2	len3	len4	len5
xl[.]com	tgt[.]org	iddm[.]org	fhqqc[.]com
gz[.]net	paf[.]org	yqqb[.]org	mseur[.]com
ed[.]org	bcc[.]com	nvso[.]net	ofddy[.]com
df[.]org	zla[.]com	nqui[.]com	agejx[.]net
wx[.]com	tgf[.]net	duth[.]net	mlngi[.]com
len6	**len7**	**len8**	**len9**
kwwezx[.]net	gbiutoj[.]com	mitsxpjh[.]com	nxbfvjkhr[.]org
bwidqv[.]com	jeihdgt[.]com	wtfmbcvt[.]com	lkhyleslk[.]net
piuxic[.]com	qspdwhc[.]com	jgggzbmq[.]org	nmshofzmh[.]net
xdgzas[.]com	grjfgpw[.]net	qqegowhv[.]org	ykbhnoers[.]com
nwfffu[.]org	vudgfcm[.]net	invphyzf[.]com	mqnbqsygn[.]org

表 *6. MyEtherWallet* キャンペーンで確認されたサンプルの偽装ドメイン

これらのキャンペーンを理解する上でいくつか抜け落ちている点の 1 つは、発見されたドメインの数がサンプルセットとして小さすぎるため、すべてのドメインに Muddling Meerkat との重複があることを確認するには不十分である可能性があるということです。しかし、この一連のキャンペーンは、中国と関連する脅威アクターがスパム活動においてドメイン偽装をどのように利用しているかを示すもう一つの例です。

その点を踏まえ、当社はスパムトラップを見直しました。

ケース #3：よく知られた恐喝キャンペーン

QR コードや日本語のキャンペーンだけでなく、よく知られたスパムの手法を利用したキャンペーンでもドメインのなりすましが見つかりました。ハッカーがユーザーのデバイスにアクセスし、由々しい行動を記録したと主張する恐喝メールは、マルスパムの世界では一般的です。これらも偽装された送信者ドメインを使用していることには少し驚きましたが、これには裏があります。攻撃者は、ユーザー自身のメールアドレスを偽装し、確認するように促すのです。メールは、ユーザーのデバイスが侵害されたことを伝え、その証拠として、攻撃者はメッセージがユーザー自身のアカウントから送信されたと主張します。しかし、実際にはその送信は行われていません。メールヘッダーは、ユーザーのものではなく、中国の IP アドレスを通じて送信されたことを示しています。電子メールの内容の例については、下の図 11 を参照してください。

メールには、デバイスからマルウェアを削除する代わりに送信者に支払いを行うようユーザーに指示し、スパムメッセージごとに異なるビットコインウォレットアドレスが含まれています。これが恐喝サービスなのか、同じ人物がさまざまなウォレットを使用しているのかは不明です。収集した例では、被害者は 1,800 米ドルの支払いを求められています。多くのユーザーが実際にこれらのスパムメールを読むことは稀であり、行動を起こすのはさらに稀かもしれませんが、この詐欺はどうやら成功しているようです。`bitref[.]com` でこれらのウォレットの残高を確認すると、かなりの資金が含まれていることがわかります。1 つのウォレットには約 26,000 米ドルが含まれていました。

こんにちは！残念ながら、あなたにとって悪いニュースがあります。以前、あなたのデバイスが私のプライベートトロイの木馬である RAT(Remote Administration Tool) に感染しました。詳細については、Google で調べてください。私のトロイの木馬は、あなたのファイル、アカウント、カメラにアクセスすることを可能にしました。このメールの送信者を確認してください。私はあなたのメールアカウントから送信しました。このメールを確実に読むために、複数回送信されます。あなたはポルノサイトを閲覧し、汚いビデオを見ながら楽しんでいます。私はあなたが（あなたのデバイスのカメラを通じて）自分を満足させているのを記録しました。その後、痕跡を残さないようにマルウェアを削除しました。私の意図を疑うなら、あなたのビデオを友人、親戚、すべてのメール連絡先、ソーシャルネットワーク、ダークネットで共有するのは簡単です。必要なのは、私のアカウントに 1800 米ドルのビットコイン（BTC）を送金することです。取引が成功したら、すべてを削除します。私は約束を守ります。ここでビットコイン（BTC）を簡単に購入できます： https://cex.io/buy-bitcoins https://nexo.com/buy-crypto/bitcoin-btc https://bitpay.com/buy-bitcoin/?crypto=BTC https://paybis.com/ https://invity.io/buy-crypto または他の交換所を Google で検索してください。その後、ビットコイン（BTC）を直接私のウォレットに送信するか、フリーソフトウェアをインストールします：Atomicwallet、または： Exodus ウォレット、受信して私のウォレットに送信します。私のビットコイン（BTC）アドレスは： 1GtGZpzfRkAVBL48F68mi8bTcatwpTZGm8 はい、それがアドレスのように見えます。私のアドレスをコピーして貼り付けてください。それは（cAsE-sEnSEtiVE）です。このメールを開いてから 3 日以内に通知されます。このメールアカウントにアクセスしたので、このメールがすでに読まれているかどうかがわかります。すべては公正に行われます。私からのアドバイスは、アカウントのすべてのパスワードを定期的に変更し、最新のセキュリティパッチでデバイスを更新することです。

図 *11.* なりすまし送信者ドメインを利用した恐喝スパムの一例

これらのキャンペーン、そしておそらく送信者ドメインを偽装した他の多くのキャンペーンは、残存するスパムボットから発信されている可能性があります。少なくとも、攻撃者は被害者のメールアドレスを確認して、スパムメールが受信または読まれていることを確認していません。受取人のメールアドレスが、2007 年に最後にコンテンツをホストし、15 年以上メールユーザーがいなかった当社のドメインの 1 つに関連付けられていた事例があります。これらのメールがトリガーされた理由を説明する侵害記録は存在せず、実際にこれらのユーザーが存在したかどうかは私たちには不明です。

この件と、当社が発見した他の同様のスパムキャンペーンは、インターネット空間に漂流する放棄されたスパムメールのキャノン砲のようなイメージを呼び起こさせます。また、古いワームが拡大していることも確認しました。これは、悪意のあるスパマーが QR コードや上記のような偽のアカウントページなどの手法に移行している間に、ボットネットの残骸が動作したまま放置されたことを示すもう 1 つの兆候です。これらのキャンペーンは、現在はおそらく自動化されており、Muddling Meerkat のような高度な攻撃者による最近の活動よりも、むしろ拡大する可能性が高いように思われます。

ケース #4：謎のマルスパム

この研究計画全体は謎から始まりましたが、この論文の最後は別の謎で締めくくられます。それは、偽装された送信者ドメインを使用し、明らかな目的のない一見無害な Excel スプレッドシートの添付ファイルを含む、非常に活発なスパムキャンペーンです。当社は、Muddling Meerkat が使用するものと同じ種類のドメインを偽装しているこれらのメールの動機を説明できる段階にはありません。

これらのメールは、上海亚凯（「Shanghai Yakai」と訳される中国の貨物会社の名前）から送信されたとされています。それぞれのメールアドレスは大きく異なり、「Edward.Evelyn」や「Heidi.Gracie」などの合成されたユーザー名が含まれています。キャンペーンは 2024 年に 3 日に 2 度ほど見られましたが、変わったところはありませんでした。件名には、メールに新しい貨物料金の更新が含まれていることが示されており、添付ファイルは「上海亚凯国际運价表 .xlsx」という名前のスプレッドシート一つです。これらのファイルには悪意のあるコンテンツは見つかりませんでした。

メールに、ボタンリンク（CTA）はありません。どう見ても、これは中国の海運会社が継続的に更新している運賃表に過ぎません。しかし、目的は何なのでしょうか。これらのメールは、メールアドレスの変更や登録解除を忘れた顧客に送信されているようには見えません。ドメイン偽装の使用は、あらゆる正当性を完全に失わせます。運送会社または悪意のある攻撃者が、このようなメールを送信するのかは不明です。表 7 は、送信者ドメインのサンプルを示しています。

len4	len5	len6	len7
igeb[.]net	accou[.]com	axegal[.]com	awpking[.]com
kwfm[.]com	drsmj[.]com	devsmx[.]com	comitis[.]com
pqhh[.]com	eddim[.]com	glypix[.]com	donmenn[.]com
rrbc[.]com	hetoo[.]com	gulart[.]net	fundsle[.]com
tkee[.]net	horek[.]com	jomila[.]net	karnege[.]com
tnmc[.]com	memsz[.]com	mzylla[.]com	mtrplay[.]com
ukei[.]net	svard[.]net	okayme[.]com	rajprem[.]com
utpz[.]com	tapli[.]net	theiwl[.]com	techsox[.]com
vbhh[.]com	uweko[.]com	vaites[.]com	tjipbpo[.]com
wuwo[.]com	youbi[.]com	ynglet[.]com	wulthur[.]net

表 7. 上海ヤカイの貨物スパムで使用されるなりすまし送信者ドメインのサンプル

個人向けスパムでも同様のキャンペーン手法が見られましたが、貨物会社からのメッセージではなく、インドの投資会社からの投資信託の価値を提供するメールです。これらのメッセージは、Google Mail によって疑わしいスパムとしてフラグが立てられており、無害なスプレッドシートと PDF ファイルも含まれています。この場合、送信者のユーザー名は以前の知人であり、そのメールアカウントはスパム操作に使用するためにハッキングされた可能性が高いようです。しかし、中国の貨物スパムのように、これらのメッセージがスパム行為者にとってどのような価値があるのかは不明です。

権威 DNS サーバーからの視点

Muddling Meerkat は、6 年以上にわたり奇妙な DNS 操作を行っています。これには、中国のグレートファイアウォールからの偽の応答や、彼らが管理していない長期間放置されたドメインの使用が含まれます。それらの DNS 活動には複数のレコードタイプが含まれますが、偽の応答はベースまたはターゲットとなるドメインの MX レコードに対するものです。たとえば、`kb[.]com` には MX レコードがないにもかかわらず、中国の IP アドレスから `kb[.]com` の MX レコードを含む DNS 応答が観測されています。さらに、これらの偽のレコードには、時間の経過とともに一度だけ観測される短いランダムなホスト名（例: `x4rd.kb[.]com`）が含まれており、これが `kb[.]com` の観測された MX レコードである可能性があります。2024 年 3 月に最初に公開した際には、このようなドメインを約 20 個特定していましたが、現在では他にも数百個のドメインが確認されています。

攻撃者によるスパム活動の証拠を探すことに加えて、当社は権威サーバーの DNS ログを分析し、所有するドメインの担保データで確認された偽の DNS 応答との照合を試みました。その仮説は、偽の MX レコードドメインの一つ、（例：`x4rd[.]our[.]domain`）に対するクエリを確認できれば、クエリ元の IP アドレスを使用して Muddling Meerkat の活動をより深く理解できるであろう、というものでした。残念ながら、Muddling Meerkat レコードを当社のサーバーのクエリと確実に一致させることはできませんでした。

この一致が見つからないことは、何を意味するのでしょうか。それは、x4rd[.]our[.]domain のような偽の MX 応答を受け取った人や物が、それを後続の DNS クエリで使用せず、スパムにも使用していないであろうことを意味します。この明確な動機の欠如は、ボットネットが偽装メールで使用するためにドメインを受け取るという概念を覆すように思われます。では、応答は何に使われているのでしょうか。わかりません。Muddling Meerkat は依然として謎です。アイデアや別の視点をお持ちでしたら、ぜひお聞かせください。

結論

Muddling Meerkat の実態を特定することはできませんでしたが、調査は最終的に成功しました。攻撃者がマルスパムでなりすましドメインを使用する方法について多くのことを学びました。これにより、それらを阻止する方法を考案することができます。私たちのような脅威研究者にとって、そうした洞察の一つ一つは、多くの場合、その背後にある意図を知ることと同じくらい重要です。

いつも欲しいものが手に入るとは限りませんが、見つかるかもしれず、必要なら手に入ります。[8]

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 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： 20241223v1