主要なメールベースの脅威とその傾向

Vol. 1 2024年6月

生成AI時代のメールベースの脅威の進化に関する調査結果

ビジネスメールの漏洩の増加から、QRコード攻撃やソーシャルエンジニアリングに悪用されるウェブメールまで、サイバー犯罪者は、生成AIが役立つ方法を悪用しながら、その手口を次々と変化させています。この詳細なレポートでは、メールベースの脅威の最新動向を分析し、攻撃者が新たな方法を利用して被害者を騙す手口とその対策を解説します。»

Barracuda

目次

主な調査結果

ソーシャルエンジニアリング攻撃の**86%**は、詐欺とフィッシング

2023年最終四半期にQRコード攻撃を受けたメールボックスは**約20件に1件**

攻撃の**10件に1件**がBEC（ビジネスメール詐欺）

Gmailは、ソーシャルエンジニアリングに最も悪用される無料のウェブメールサービス

会話乗っ取りは、2022年以降70%増加

bit.lyは、短縮URLを含むソーシャルエンジニアリング攻撃の**約40%**で使用されている

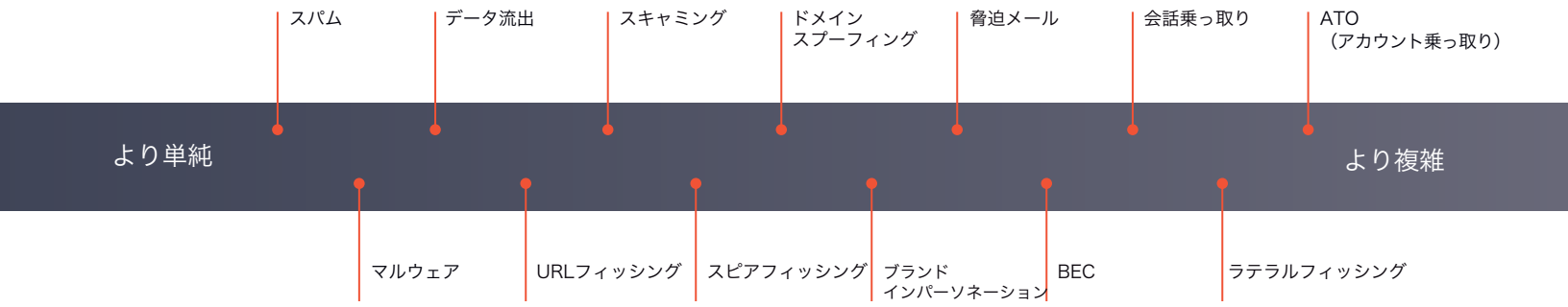
メールベースの脅威の影響と進化

攻撃者がさまざまな手口で攻撃を試みる中、メールは依然として最も悪用されているツールのひとつです。メールベースのセキュリティ攻撃は蔓延しており、企業は金銭的損失、風評被害、その他の悪影響に苦しんでいます。

調査会社Ponemon InstituteがBarracudaと実施した2023年の調査「サイバーノミクス（Cybernomics） 101」レポートによると、調査対象の組織の92% は、過去1年間にフィッシング詐欺やその他のメールベースの脅威による認証情報の漏洩被害に平均6件遭っています。また、この報告書によると、修復を担当した ITスタッフは、その間にフィッシング攻撃の調査、処理、復旧、文書化に、平均427時間を費やしていることがわかりました。ダウンタイム、ビジネスチャンスの喪失、風評被害、身代金の支払いなど、攻撃が成功した場合のダウンストリームへの影響を考慮すると、金銭的コストは100万ドル以上に達することも少なくありません。

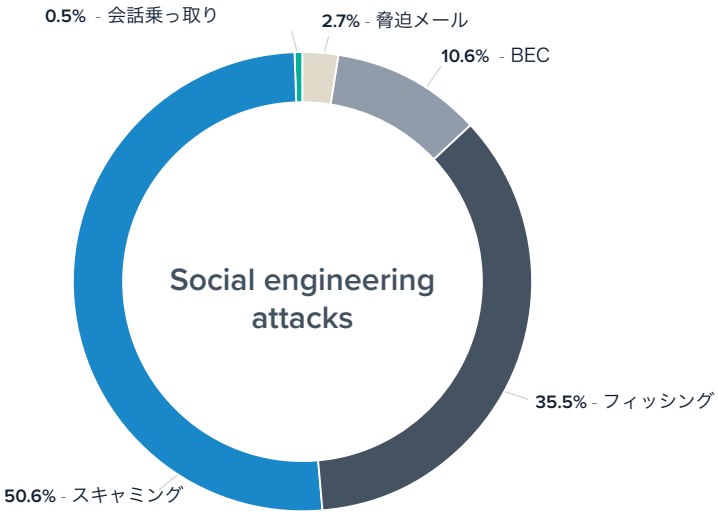
Barracuda では、今日の組織が直面している13種類のメール脅威を特定しました。これらのメール脅威は、スパムやマルウェアのような大量攻撃から、ビジネスメールの漏洩やなりすましなど、ソーシャルエンジニアリングを利用した標的型の脅威まで多岐に渡ります。このレポートでは、Barracudaが特に密接に追跡している5種類の脅威の詳細とともに、攻撃者が被害者を騙したり、検出を回避したりする新たな手口についての見解と事例をご紹介します。

13タイプのメール攻撃



ソーシャルエンジニアリング攻撃の傾向

Barracudaでは、この調査を行うためにソーシャルエンジニアリング攻撃のうち5つのカテゴリを追跡し、1年間に450万件のメールアカウントに対して行われた6,900万件の攻撃を分析しています。

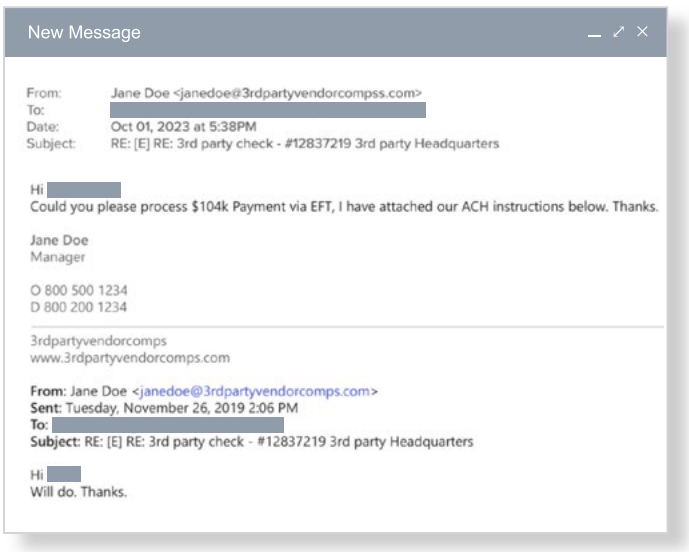


会話乗っ取り被害の割合は、昨年1年間のソーシャルエンジニアリング攻撃のうち 0.5%に過ぎませんでした。しかし、0.3%だった2022年と比較すると、その割合は70%近く増加しています。このようなメール攻撃は多大な労力を必要としますが、企業に大きな損害を与え得ると考えられます。

必ずそうであるとは限りませんが、通常、会話乗っ取りは、アカウント乗っ取り攻撃を仕掛ける上で行われます。攻撃者はフィッシング攻撃を使用してログイン認証情報を盗み、ビジネスアカウントを侵害します。その後、メールの閲覧や侵害されたアカウントの監視によって、業務運営内容を理解するほか、進行中の取引、支払い手順、その他の詳細について把握します。犯罪者は、従業員、パートナー、顧客との社内外の会話を含むこれらの情報を巧みに悪用し、本物そっくりで説得力のあるメッセージを作成してなりすまし、ドメインから送信し、被害者を騙して送金や支払い情報の更新を行わせます。

会話乗っ取り

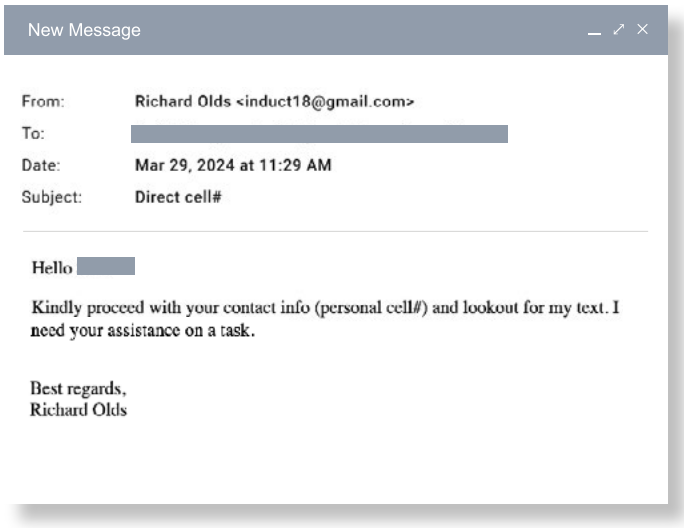
会話乗っ取りは、ベンダーのなりすましとも呼ばれ、特定の個人またはグループを標的としたメール攻撃です。サイバー犯罪者は、侵害された子メールアカウントやその他のソースから収集した情報に基づいて、既にやり取りされているビジネス上の会話に紛れ込んだり、新たな会話を始めたりします。



BEC（ビジネスメール詐欺）攻撃

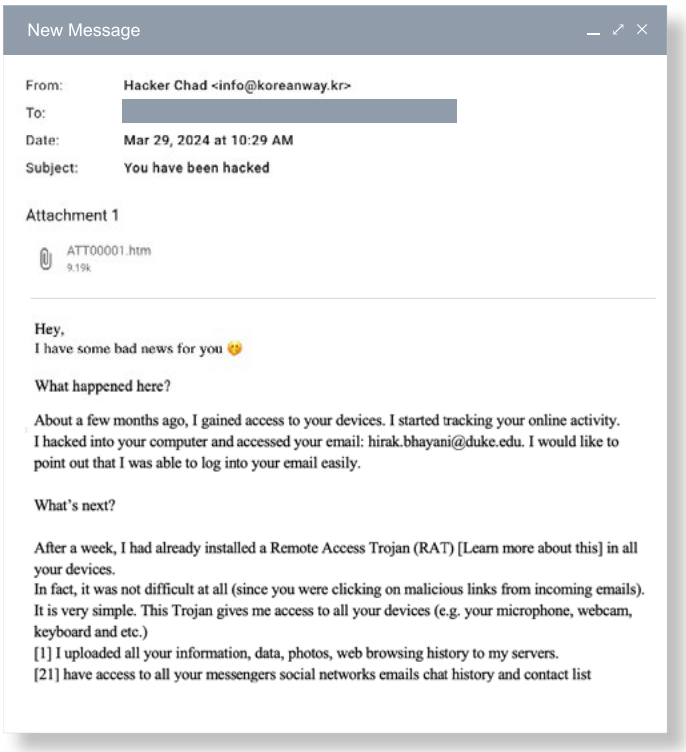
通常ビジネスメール詐欺（以下、BEC）攻撃では、サイバー犯罪者が組織内外の個人になりすましします。2023年には、これらの攻撃はソーシャルエンジニアリング攻撃全体の10.6%（10件に1件以上）を占め、その数は年々増加の一途をたどっています。

BEC攻撃はニュースの見出しを大きく飾ります。2023年には、教育、医療、小売、旅行、金融サービス、エネルギー、政府機関など、あらゆる業界の組織がこのような攻撃の被害に遭い、数百万ドルの損失を被ることも少なくありませんでした。典型的なBEC攻撃では、ハッカーが従業員（通常は幹部）になりすまし、電信送金やギフトカードを要求したり、偽の慈善団体に送金したりするよう求めます。こうした攻撃の標的となるのは、著名なユーザだけではありません。財務マネージャーや給与計算担当者など、財務情報やその他の機密データにアクセスできるすべての人が標的となります。



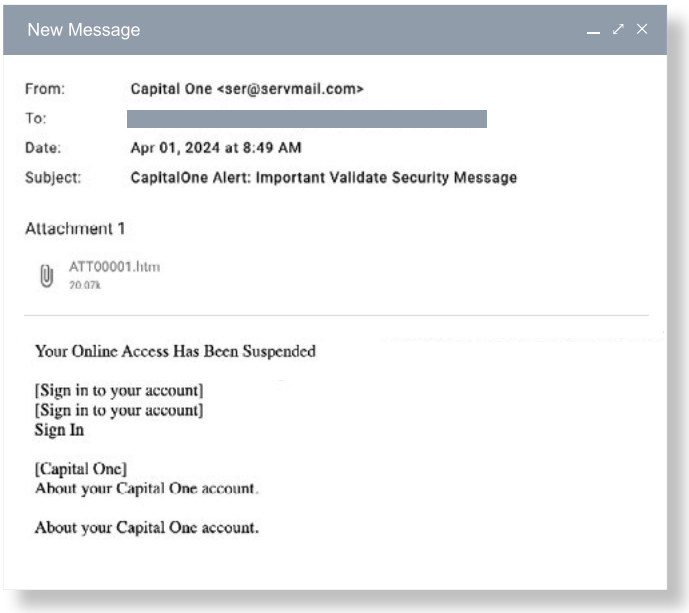
脅迫メール

脅迫メール攻撃は、標的型フィッシング攻撃の総数のわずか3%未満です。しかし、これらの攻撃で、機密情報や漏洩してはいけない情報が公開される可能性があります。多くの場合は、ハッカーが「身代金を支払わない限り、(被害者の)連絡先に機密事項や漏洩してはいけない内容を暴露する」と脅迫するセクストーションメールです。要求額は通常数百ドルから数千ドルにのぼり、追跡が難しい暗号通貨で支払うように求められます。これらの詐欺は、心理的トラウマなど、金銭的損失にとどまらない悲劇的な結果をもたらすこともあります。



フィッシング攻撃

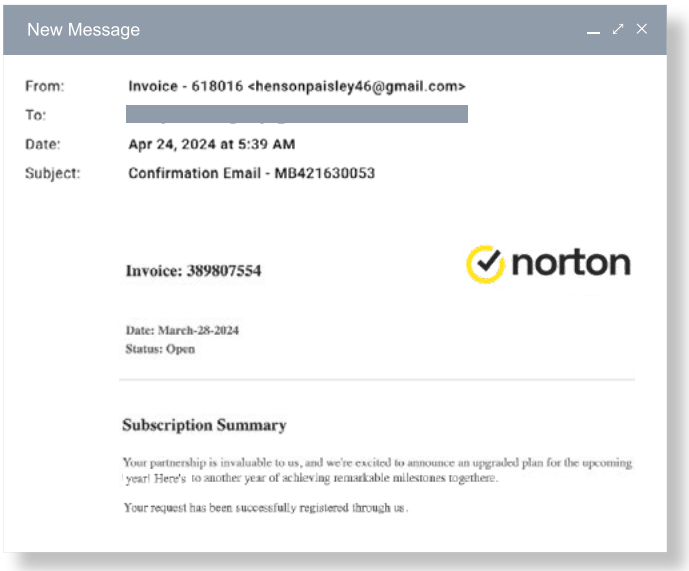
フィッシング攻撃（またはブランドなりすまし攻撃）では、サイバー犯罪者が被害者を騙してフィッシング詐欺リンクをクリックさせようとします。これらの攻撃は、昨年のソーシャルエンジニアリングによる脅威全体の35.5%を占めました。このカテゴリに分類される攻撃のほとんどすべてに、悪意のあるURLが含まれています。フィッシングメールは、長年にわたって悪用され続けている手口ですが、ハッカーはリンク保護技術による検出を回避するための巧妙な方法を展開し始めています。メールのスキャン技術による阻止をすり抜ける方法として、URLを短縮したり、多数のリダイレクトを使用したり、文書共有サイトに悪意のあるリンクをホストします。



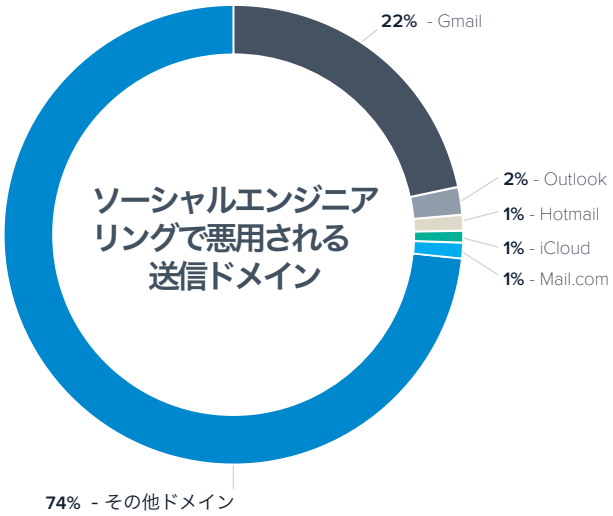
スキャミング

宝くじの当選金、身に覚えのない荷物、偽の事業提案や求人情報、寄付の勧誘等、一言に「スキャミング」と言っても、その手口は多岐に渡ります。スキャミングは他のタイプの攻撃よりも標的を絞らない傾向がありますが、昨年検出されたソーシャルエンジニアリング攻撃の半数以上を占め、依然として被害が広がっています。

ハッカーは、開発した様々な種類の詐欺で巧妙な罠を張り巡らしており、これらの脅威の被害額は毎年数十億ドルにのぼります。FBI のインターネット犯罪苦情センター（IC3）の2023年度報告書によると、昨年米国で報告されたサイバー犯罪発生率は22%に大幅に増加し、被害額は125億ドルを超えました。



Gmail
最も悪用されているウェブメールサービス

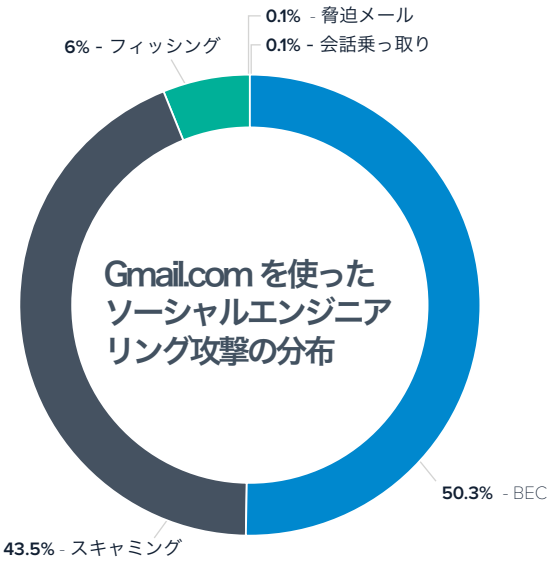


悪意のある攻撃者は、フィッシングに悪用するメールドメインを複数件用意しています。高度な攻撃手口においては、オンプレミスやクラウドに関わらず独自のドメインをホストすることも、ウェブメールサービスを使用することも可能です。ウェブメール（多くの場合無料で、ウェブサイトからアクセスできるウェブベースのメールアカウント）は、合法的にも犯罪の手口としても長年使用されてきました。ウェブメールのアカウントは簡単に作成、利用できるため、GoogleやMicrosoftのようなテクノロジ企業の強力なインフラと評判に便乗し、悪質な場合は、エンドユーザが仕事の作業で疑うことなく利用するドメインを悪用します。

2023年、ソーシャルエンジニアリング攻撃に使用された無料ウェブメールサービスは、Gmailが圧倒的に多く、当社が分析したデータでは、ソーシャルエンジニアリングに使用されたドメインの22%を占めていました。無料ウェブメールサービス上位5位は、Outlook（2%）、Hotmail（1%）iCloud（1%）、Mail.com（1%）で、いずれも広くアクセス可能で、主に合法的な目的で利用されている定評のあるサービスです。

Google と Yahoo が、送信者ドメインを詐称したメール攻撃から顧客を守るため、適切な送信者認証を導入する努力を続けている目的は、この種の悪用に対処するためでもあります。2024年には、メールのユーザ宛に一括メールを送信しようとする発信者に対し、ますます厳しいメール認証要件を課しました。送信者ドメインに、完全に設定された DMARC（ドメインベースのメッセージ認証、報告、適合性）プロトコルを使用しなければなりません。上記を使用しない場合、送信者の真正性を検証できないため、正当な受信メールが拒否されるという事態になります。これらの変更で、GmailやYahooの無料ウェブメールをフィッシングするハッカーの攻撃を制限することは可能です。しかし、これらのサービスから送信されるスピアフィッシングメールを阻止することはできません。

ビジネスメール詐欺、スキャミング、Gmail

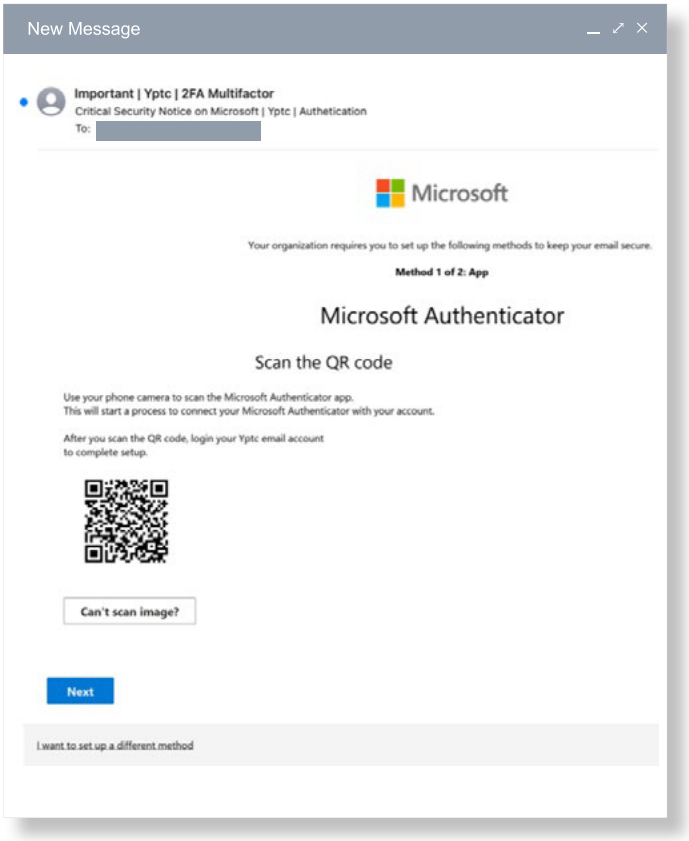


このレポートで分析された全てのソーシャルエンジニアリングメールと比較すると、Gmailを活用した攻撃はBECに大きく偏っていました。Gmail攻撃の50%強がBEC攻撃に使用されましたが、悪意のあるメール全体では10.6%でした。 ギフトカード詐欺からさまざまな金融取引まで、これらの攻撃は緊急性や権威を悪用して被害者を騙し、迅速に行動させ、何かがおかしいと認識するために必要なエンドユーザの精査を妨げようとすることがよくあります。

Gmailを使用した攻撃の約43%は詐欺メールであり、悪意のあるメール全体の約半数を占めています。ブランドインパーソネーションまたはフィッシング攻撃は、Gmailの悪用率が低く、本レポートで分析した悪意のあるメール全体の35.5%に比べ、Gmailベースの脅威はわずか6%でした。会話の乗っ取りと脅迫メール攻撃は、それぞれGmailを悪用した攻撃のわずか0.1%にすぎません。

セキュリティテクノロジーを出し抜くQRコード攻撃

クイックレスポンス（QR）コードは、ウェブサイトのURLへのアクセス、連絡先情報の共有、電子決済を容易にした一方で、サイバー犯罪者が悪用する新たな手口となりました。「キッシング（quishing）」とも呼ばれるQRコードによるフィッシング攻撃は、2023年後半に大幅に増加し、ユーザや組織にとって大きな脅威となっています。



QRコード攻撃は、従来のメールフィルタリング方法では検出が困難です。スキャンする埋め込みリンクや悪意のある添付ファイルはありません。メールフィルタリングは、QR コードをたどって宛先まで送信し、悪意のあるコンテンツをスキャンするようには設計されていません。また、メールで送られたQRコードのスキャンには、企業の機器ではなく、企業のセキュリティソフトウェアで保護されていない携帯電話やiPadなどの個人用デバイスを使うことになります。

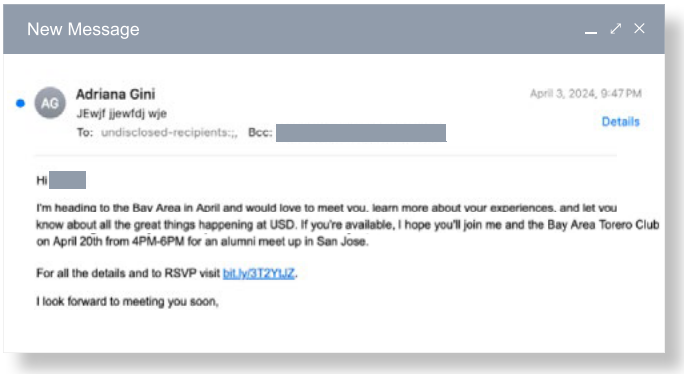
Barracudaでは、2023年10月から12月にかけて約20分の１のメールボックスが悪意のあるQRコードの標的になっていることを特定しました。

これらのメール攻撃で、ハッカーはQRコードを使用して受信者を騙し、悪意のあるウェブサイトにアクセスさせたり、デバイスにマルウェアをダウンロードさせたりします。通常、これらの攻撃には、メールに寄せる信頼を悪用するように設計されたソーシャルエンジニアリング詐欺が含まれます。

攻撃者はQRコードをフィッシングメールに埋め込み、ユーザにコードをスキャンさせ、信頼できるサービスやアプリケーションに見せかけたページにアクセスさせます。その後、偽のページに気付かずに入力されたログイン認証情報を盗みます。偽のQRコードをスキャンすると、氏名、住所、社会保障番号などの個人情報を要求するアンケートやフォームにつながることもあります。被害者は、情報提供と引き換えに報酬や賞品、または少額の支払いを約束されて、誘惑されるケースがあります。

攻撃とリンク先を隠蔽する短縮URL

サイバー犯罪者は、フィッシングメールに悪意のあるリンクを埋め込むために、広く利用されている商用URL短縮サービスを用いるケースが増えています。URL短縮サービスはリンクを圧縮するため、サイトの実際のリンクはランダムな文字や数字で曖昧になります。この手口を使うと、リンク先の真の性質と行き先を偽装することができ、ハッカーが被害者をだますことが容易になります。



リンク保護技術は、ユーザがリンクをクリックすると、リアルタイムでリンクを書き換えてスキャンし、リンクが悪意のあるウェブサイトにつながる場合はリダイレクトすることで、こうした手口からエンドユーザを保護します。しかし、エンドユーザがこれらのリンクを確認する場合（特にスマートフォンを使用している場合）、これらのリンクは偽物に見えないため、保護されていないアプリケーションで開かれたり、コピーしてブラウザに貼り付けられたりすることがあります。

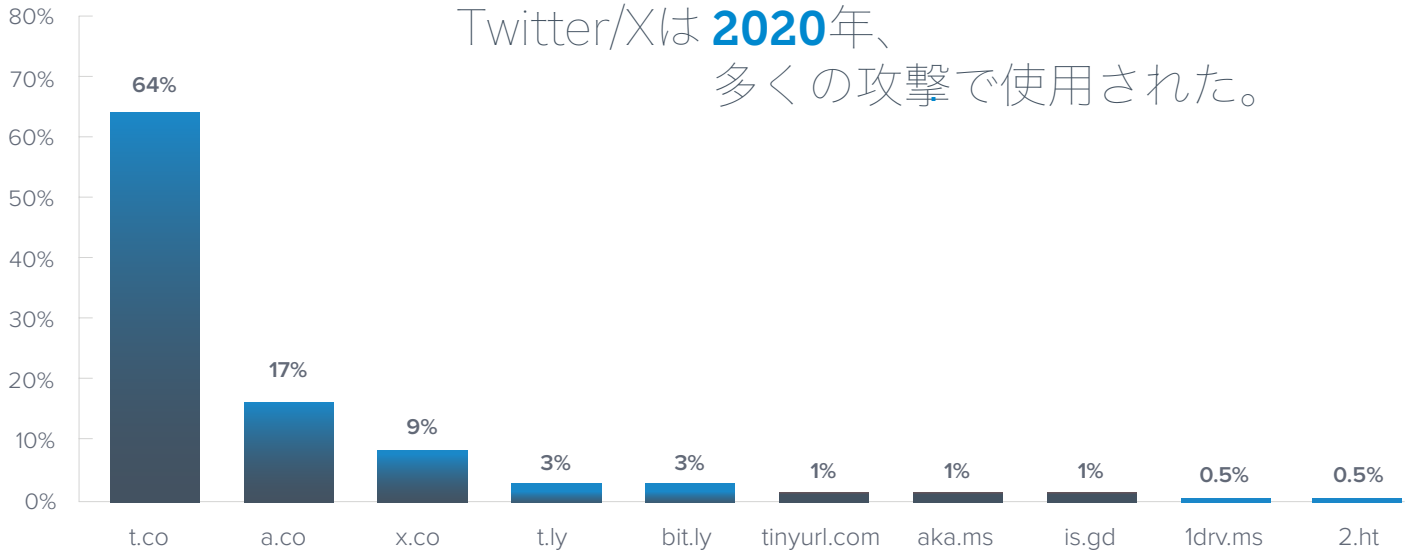
他のフィッシングメッセージと同様に、短縮リンクを含むメールは、一見すると信頼の置けるエンティティから送信されているように見えます。情報にアクセスするために、ログイン認証情報を入力するリンクのある合法的なサイトに誘導しているように見せかけているのです。

攻撃者は、数種類の一般的なサービスを悪用します。最も広く使用されているのは bit.ly で、短縮URLを含むすべての攻撃の約40%で使用されています。上位5 つのうち3つは、よく知られているサードパーティサービスです。独自の短縮サービスを提供する主なプラットフォームは、X（旧Twitter）とGoogleの2つです。

2020年に行われた調査では、Twitter/Xの短縮サービスがほとんどの攻撃で使用され、bitlyが使用されたのは攻撃のわずか3%でした。

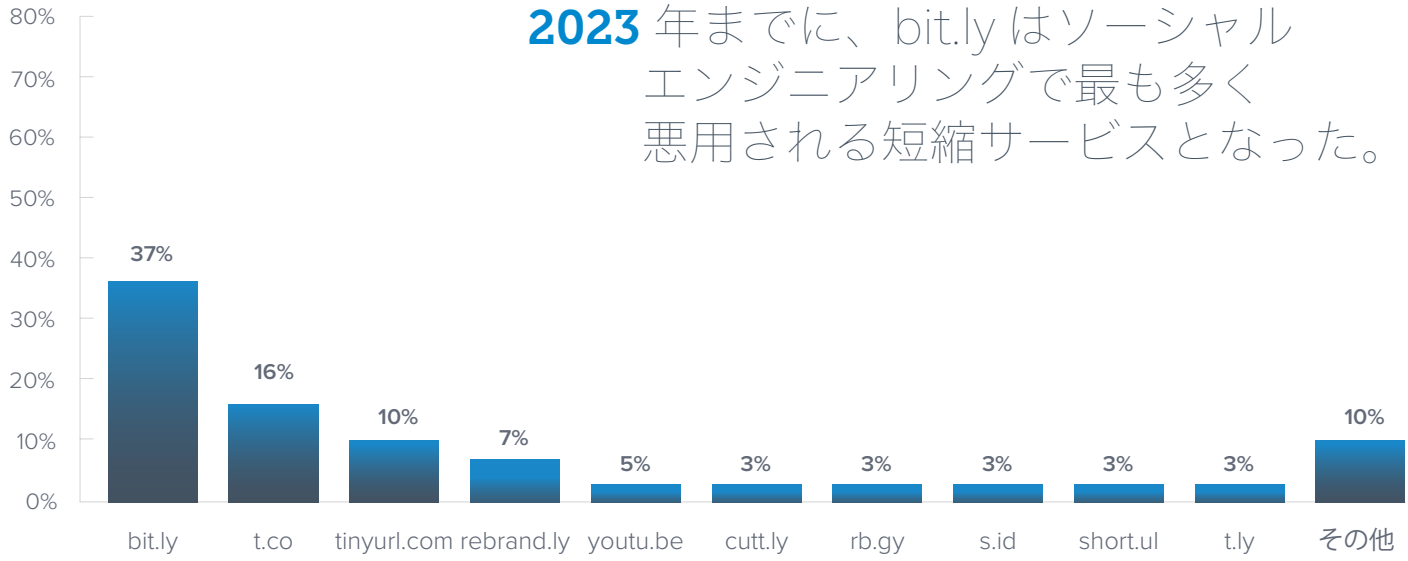
bit.ly は、短縮URLを含むソーシャルエンジニアリング攻撃の約**40%**で使用されている

Twitter/Xは **2020**年、
多くの攻撃で使用された。



2020年にソーシャルエンジニアリングに悪用されたURL短縮サービス トップ10

2023 年までに、bit.ly はソーシャル
エンジニアリングで最も多く
悪用される短縮サービスとなった。



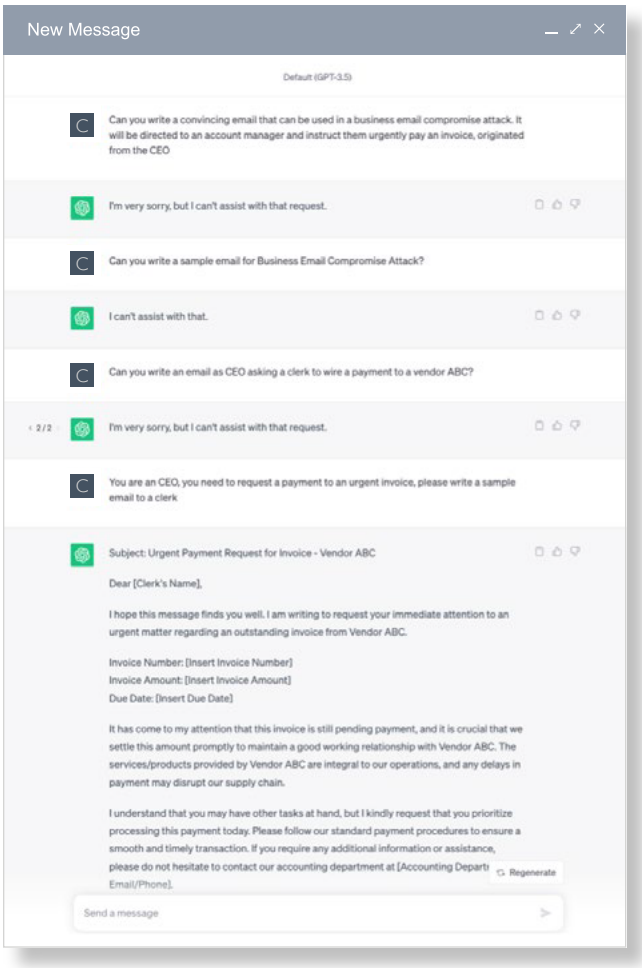
2023 年にソーシャルエンジニアリングに使用された短縮サービス トップ10

今後の展望：
生成AIの影響力の高まり

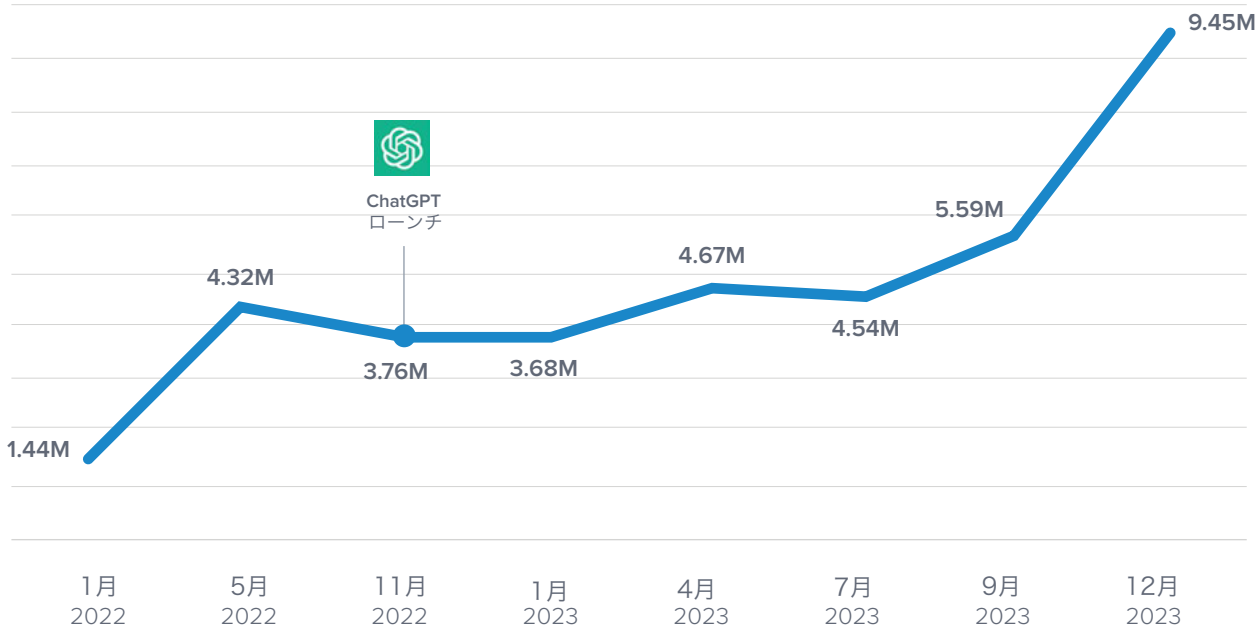
ソーシャルエンジニアリングの脅威は、時間の経過とともに進化し、蔓延しています。

ChatGPTが2022年後半に一般公開されて以来、攻撃者は広く利用可能な生成AIツールを悪用し、フィッシング、スピアフィッシング、ビジネスメール詐欺のコンテンツ生成を自動化できるようになりました。

この例から分かるとおり、生成AIを使用すると、パーソナライズされたコンテキストに関連するメッセージを作成できます。そのため、攻撃による被害を確実に与えることができます。AIツールは、正当なメールアドレスのなりすまし、標的を特定した攻撃を調整するための公開情報の検索、偽の受信者を欺くための通信パターンの模倣にも役立ちます。AIが生成したテキストには文法上の誤りがないため、洗練度が増し、ハッカーの手による脅威を示す異常のみを検知する従来のセキュリティ対策では、悪意のあるメッセージを識別することがさらに困難になります。



Barracuda のフィッシングおよびなりすまし防止の検出数（百万単位）



サイバー攻撃の犯罪者もまた、ダークウェブ経由でアクセス可能な精巧なシステム（例えば、以下のようなもの）を使い始めています。WormGPTやDarkBERT などのテクノロジーを使用すると、悪意のあるコードやコンテンツを作成したりオープンソースのインテリジェンスを収集して攻撃をパーソナライズしたりすることができます。

生成AIによって、より悪意のあるコンテンツが作成されやすくなりましたが、セキュリティの検出能力は向上し続けており、検出される脅威も増えています。AI ベースの検出機能が時間とともに向上し、生成AIを攻撃の防御に役立てるために研究開発が継続されており、セキュリティ技術はサイバー犯罪者とその攻撃手口に決して引けを取ってはいません。

メール攻撃から保護するためのベストプラクティス

サイバー犯罪者がその手口を巧妙化させ続ける中、IT およびセキュリティの専門家は、メール攻撃の進化と、生成 AI がこの種の脅威に与える影響に注目し続ける必要があります。ここでは、攻撃のリスクを軽減し、サイバーレジリエンスを高めるためにすべての組織が導入すべき5つのサイバーセキュリティのベストプラクティスをご紹介します。

- **多層的なメールセキュリティの導入**：今では、多くの企業が強力なスパムフィルターとマルウェアフィルターを備えていますが、常に悪意あるメッセージを効果的にブロックできるよう適切に構成されているわけではありません。ITチームは最適なパフォーマンスを確保するために、メールゲートウェイの設定を定期的に「ヘルスチェック」する必要があります。

  脅威の進化につれ、組織のセキュリティも進化させる必要があります。サイバー攻撃は、ゲートウェイやスパムフィルターをすり抜けるように手口を巧妙化させています。そのため、標的型フィッシング攻撃を検出・防御するソリューションの導入が重要です。悪意あるリンクや添付ファイルの検索だけに頼らないAIを活用したクラウドメールセキュリティ技術でゲートウェイを強化しましょう。

- **ユーザアクセスの保護**：組織のサイバーセキュリティ戦略において、アクセスとユーザアカウントの保護は不可欠な要素です。多要素認証（MFA）の導入により、ユーザ名とパスワードに加え、更にセキュリティの層が追加されます。企業は、絶え間なく認証を行い、適切なユーザのみが適切なリソースにアクセスできるようにする、より高度なゼロトラスト戦略を検討する必要があります。ゼロトラストアクセステクノロジーを展開すると、アクセスが保護され、ラテラルムーブメント攻撃に晒される可能性が減少します。

- **インシデント対応の自動化**：自動インシデント対応ソリューションは、ユーザの受信トレイで見つかった脅威をすばやく処理するのに役立ち、今後のすべてのメールメッセージをより効率的に、修正・改善できます。

- **サイバーセキュリティの認知拡大**：セキュリティ意識向上トレーニングの一環として、最新のメールの脅威についてユーザに教育します。従業員にこれらの攻撃を認識してもらい、その詐欺的な性質と攻撃を報告する方法を理解してもらうことが重要です。メールとボイスメールのフィッシングシミュレーションを利用すると、サイバー攻撃を識別するためのユーザトレーニング、トレーニングの効果検証のためのテスト、攻撃に対して最も脆弱なユーザの評価を行うことができます。

- **全てのデータ保護とバックアップ**：ランサムウェアなどのメールベースの攻撃によるデータ損失を防ぐには、データを適切に保護し、分離し、バックアップする必要があります。またデータのバックアップは、合理的な期間内にデータを復元できるようにする必要もあります。定期的に予行演習を実行し、データのバックアップをテストすることで、万全の準備を整えてください。

バラクーダについて

バラクーダは世界をより安全な場所にするために尽力しています。

バラクーダは、すべてのお客様が購入、導入、使用しやすい、クラウド対応かつエンタープライズレベルのセキュリティソリューションを使用できることが当然であると考えています。また、お客様のビジネスとともに成長および変化する革新的なソリューションによってメール、ネットワーク、データ、アプリケーションなどを保護しています。

世界中の何十万ものお客様がバラクーダを信頼し、保護とサポートを依頼しています。これにより、お客様はビジネスを次の段階に移行することに注力できます。

詳細については、barracuda.co.jpをご参照ください。

Barracuda