スピアフィッシング:
主要な攻撃と攻撃トレンド

Vol. 2 2019年8月

メールアカウント乗っ取り攻撃:
ラテラルフィッシング攻撃の防止

ラテラルフィッシング攻撃は
攻撃者がメールアカウント乗っ取り攻撃で
乗っ取った正規のアカウントを悪用する
効果的な方法として新たに実行されています。
このレポートでは、攻撃者が悪用する
最新の技術、およびビジネスを保護する
方法について詳細に説明しています。»

Barracuda
Your journey, secured.

目次

メールアカウント乗っ取り攻撃

拡散および高度化する攻撃の防止»

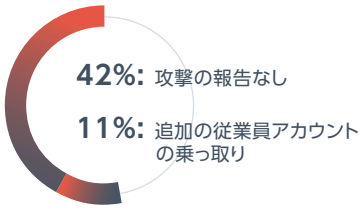
この1年、バラクーダの調査担当者は、カリフォルニア大学バークレー校およびサンディエゴ校の主要な調査担当者と協力して、企業への増大する脅威、つまりメールアカウント乗っ取り攻撃を調査しました。メールアカウント乗っ取り攻撃では、攻撃者は、正規の企業アカウントを乗っ取って、社内の連絡先から社外のパートナーまでの多くの受信者にラテラルフィッシングメールを送信します。

攻撃者は、正規のアカウントからラテラルフィッシングメールを送信するため、多くの既存のメール保護システムを効果的にバイパスし、無防備なユーザをだますことができます。このレポートでは、約100社にわたって、ラテラルフィッシング攻撃の拡散する危険な性質について詳細に説明しています。また、攻撃者が攻撃対象の受信者と攻撃で悪用するメッセージを選択する複数の方法を分析しており、この進化する攻撃に見られる高度化とステルス性に注目しています。

主な調査結果

7分の1: 攻撃を受けた企業

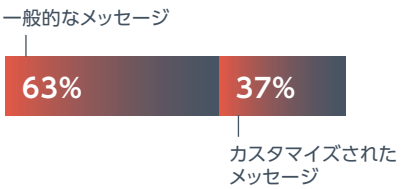
メールアカウント乗っ取り攻撃とラテラルフィッシング攻撃は企業への増大する脅威を表しています。企業を無作為に抽出した結果によると、**7分の1**が7か月以内にラテラルフィッシング攻撃を受けています。この攻撃を受けた企業の**60%**以上が**複数回の攻撃を経験**しています。



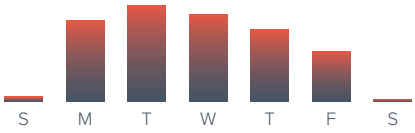
メールアカウント乗っ取り攻撃は、正規の企業アカウントを乗っ取るため、効果的で巧妙です。攻撃の11%以上では、追加の従業員アカウントが乗っ取られています。また、**42%**以上は、**受信者からITチームまたはセキュリティチーム**に報告されていません。

ラテラルフィッシング攻撃を実行する攻撃者は、4つの主要な方法に従って、攻撃対象の受信者を選択します。バラクーダの調査では、この**攻撃の55%**以上は乗っ取られたアカウントと個人的な関係または仕事上の関係がある受信者を攻撃しています。

虚偽のメッセージ

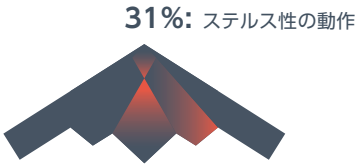


ラテラルフィッシング攻撃は、2つの一般的なメッセージである「アカウントエラー」と「共有ドキュメント」を悪用して、受信者をだまします。ラテラルフィッシング**攻撃の63%**では一般的なメッセージが悪用されていますが、**37%**では受信者の企業向けにカスタマイズされたメッセージが悪用されています。



ほとんどの攻撃
勤務時間中に実行

ほとんどのラテラルフィッシング攻撃は受信者の通常の勤務時間中に実行されています。メールアカウント乗っ取り攻撃は、リモートの攻撃者が実行している可能性があります。



バラクーダの調査では、メールアカウント乗っ取り攻撃の約3分の1は、受信者の質問に積極的に返信する、乗っ取ったアカウントからフィッシングメールのすべての痕跡を手動で削除するなど、**ラテラルフィッシングメールのステルス性と説得力を向上するように設計された追加の動作を実行しています。**

メールアカウント乗っ取り攻撃の規模

メールアカウント乗っ取り攻撃は、拡散する効果的な攻撃であるため、企業が防止する必要があります。以前のThreat Spotlightで注目したとおり、バラクーダの調査担当者が数十社のお客様を無作為に抽出した結果によると、**7分の1**が7か月以内にメールアカウント乗っ取り攻撃とラテラルフィッシング攻撃を受けています。さらに悪いことに、メールアカウント乗っ取り攻撃を受けたほとんどの企業は複数回のラテラルフィッシング攻撃を経験しています。**このような企業の60%**以上では、攻撃者が複数の従業員アカウントを乗っ取って、ラテラルフィッシング攻撃を実行しています。

ラテラルフィッシング攻撃は、乗っ取られた正規のアカウントから実行されるため、巧妙であることが判明しています。このため、多くのユーザと既存のメール保護システムはラテラルフィッシングメールを正規のものと見なします。ラテラルフィッシングメールは、従来のフィッシングメールと異なり、なりすましアカウントからも外部アカウントからも送信されないためです。バラクーダの調査担当者は、このレポートで**180回のラテラルフィッシング攻撃**を調査し、**攻撃の11%**以上で追加の従業員アカウントが乗っ取られていると推測しています。また、42%以上が受信者からITチームまたはセキュリティチームに報告されていないと推測しています。

攻撃対象の受信者を選択する複数の方法

攻撃者は調査データ全体で合計154の企業アカウントを乗っ取ってラテラルフィッシング攻撃を実行しました。バラクーダの調査担当者は、ラテラルフィッシングメールを受信した受信者を調査し、攻撃者が攻撃対象の受信者を選択する4つの主要な方法を特定しました。

1. アカウント非依存（45%）

アカウント乗っ取り攻撃の45%では、攻撃者は、乗っ取ったアカウントと何らかの関係があるアカウントではなく、可能なかぎり多くのアカウントを乗っ取ることを重視しています。

2. 攻撃対象の受信者

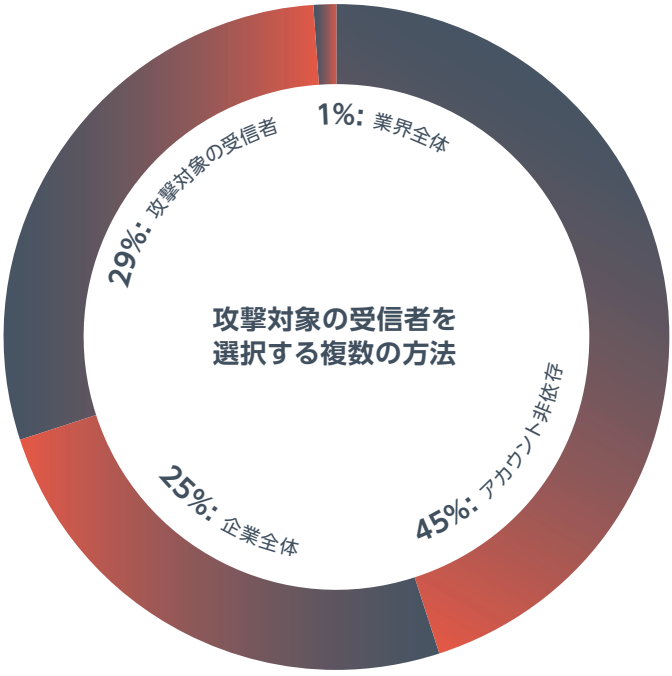
攻撃者は、乗っ取ったアカウントの最近の連絡先を取得して、攻撃対象の受信者を選択しています。攻撃の29%が、この方法に従っています。

3. 企業全体

攻撃者は、乗っ取ったアカウントを悪用して、そのアカウントの数十～数百の同僚にフィッシングメールを送信しています。攻撃の25%が、この方法に従っています。

4. 業界全体

攻撃者は、乗っ取ったアカウントを悪用して、そのアカウントの企業が属する業界の他社（ビジネスパートナーなど）の従業員にフィッシングメールを送信しています。攻撃の1%が、この方法に従っています。



ラテラルフィッシング攻撃で悪用されているメッセージ

攻撃者は、メールアカウント乗っ取り攻撃で正規のアカウントを乗っ取るため、
乗っ取ったアカウントの連絡先メールアドレスを取得して、高度な標的型メッセージを作成できます。
バラクーダの調査担当者が調査したラテラルフィッシング攻撃のほとんどからは、
下記の2つの虚偽のメッセージが悪用されていることが判明しています。

1. メールアカウントに問題があるという虚偽のアラートを含むメッセージ
2. 虚偽の共有ドキュメントへのリンクを含むメッセージ

いずれのメールの場合も、攻撃者は受信者にクリックさせるリンクを添付しています。攻撃者は、このリンクをクリックすると、正規のログインページを偽装して最終的に受信者のユーザ名とパスワードを盗み出すように設計されたフィッシングサイトに誘導される場合が多いです。

調査した攻撃の**63%**では、一般的なメッセージである「アカウントエラー」と「共有ドキュメント」(例:新しい共有ドキュメントがあります。)が悪用されています。一方、**30%**では、受信者の企業向けにカスタマイズされた高度なメッセージ(例:勤務スケジュールが更新されました。チームに伝達してください。)が悪用されています。

最も高度な方法である7%は乗っ取ったアカウントが属する企業に固有の高度な標的型メッセージを悪用しています。たとえば、あるメールアカウント乗っ取り攻撃では、攻撃者は25周年を祝おうとしている企業のアカウントを乗っ取っています。攻撃者は、乗っ取ったアカウントを悪用して、25周年の祝賀イベントを広告するそのアカウントの同僚に数十件のスピアフィッシングメール(例:FooCorpの25周年に関する添付のお知らせをご参照ください。)を送信しています。

ラテラルフィッシングメールでよく使用されている
上位10個の単語

ドキュメント (89回)

表示 (76回)

添付 (56回)

クリック (55回)

署名 (50回)

送信 (44回)

確認 (43回)

共有 (37回)

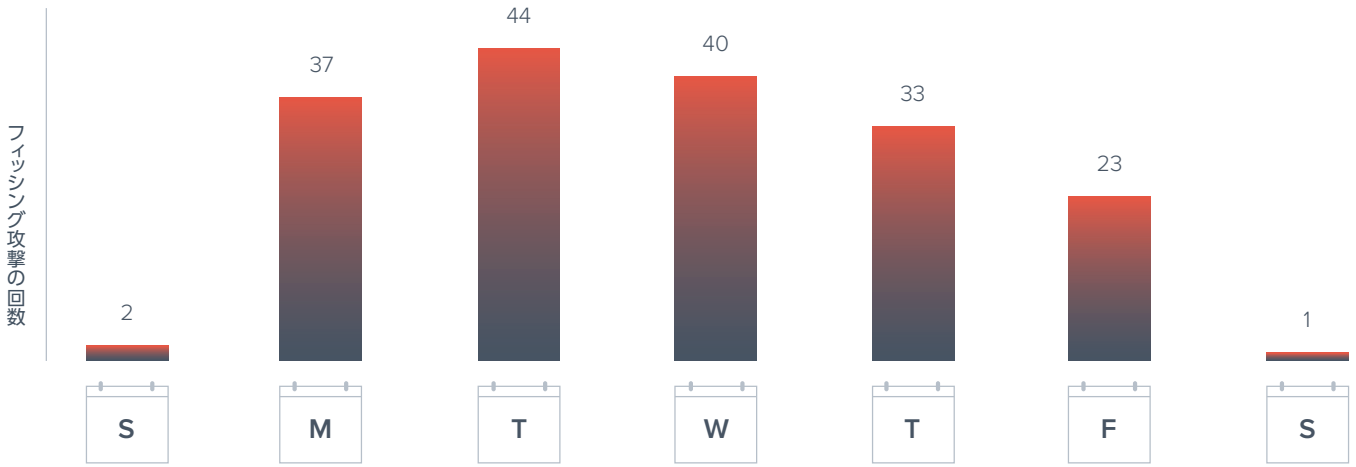
アカウント (36回)

アクセス (34回)

攻撃のタイミング

複数の調査では、通常とは異なる回数で送信されている疑わしいメールを検索すると、
フィッシングなどの攻撃を検出できる可能性があると仮定されています。
しかし、このレポートで調査された攻撃では、攻撃者は、攻撃した企業の通常の勤務時間中に、
乗っ取ったアカウントからラテラルフィッシングメールを送信していると思われます。

ラテラルフィッシング攻撃の98%は平日に実行されています。このレポートでは、ラテラルフィッシングメールの送信時間と乗っ取られたアカウントによる仕事上のメールの送信時間を比較して、ラテラルフィッシングメールが通常とは異なる時間に送信されているかどうかも分析しています。バラクーダの調査担当者によるこの分析からは、攻撃者が乗っ取ったアカウントの通常の勤務時間中に**ラテラルフィッシング攻撃の82%**を実行していることが判明しています。



高度化とステルス性

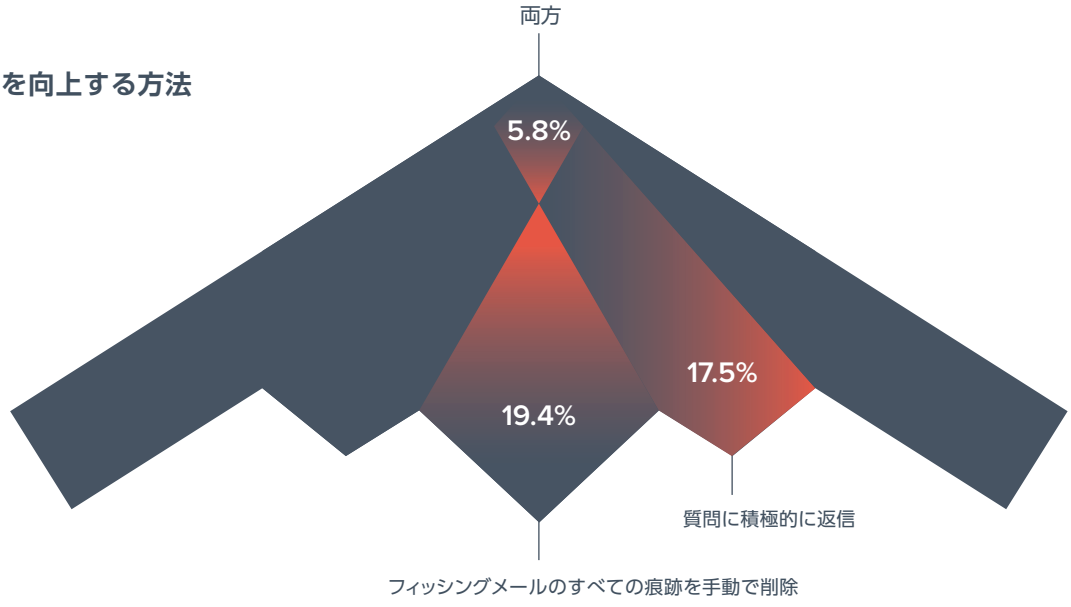
バラクーダの調査担当者によると、このレポート全体では、
ラテラルフィッシング攻撃を実行する**攻撃者の約3分の1（31%）**が、高度な方法を悪用して、
フィッシングメールの効果を向上し、攻撃の証拠を隠蔽しています。

ラテラルフィッシングメールの受信者は、乗っ取られたアカウントに返信して、メールが正規、つまり自分あてのものかどうかを確認する場合が多いです。バラクーダが調査した**乗っ取られたアカウントの17.5%**では、攻撃者は、受信者の質問に積極的に返信して、メールが正規のものであり、開いても安全であると受信者に信じ込ませています（例:ボブさん、このドキュメントは、Xに関するものです。開いても安全です。メールアドレスとパスワードでログインすると、表示できます。）。

乗っ取られたアカウントの19.4%は、受信者とやりとりし、信じ込ませるのではなく、乗っ取ったアカウントからフィッシングメールのすべての痕跡を手動で削除しています。また、送信したフィッシングメールだけでなく、質問した受信者からの返信も削除しています。

乗っ取られたアカウントの5.8%は上記の両方の高度な方法を悪用しています。

フィッシングメールの効果を向上する方法



ラテラルフィッシング攻撃の防止方法

ラテラルフィッシング攻撃を防止するには、3つの対策、つまりセキュリティ意識トレーニング、高度な検出技術、および2FA（2要素認証）が不可欠です。

1. セキュリティ意識トレーニング

セキュリティ意識トレーニングを向上し、ユーザを教育することは、ラテラルフィッシング攻撃のリスクを軽減するために役立ちます。ラテラルフィッシング攻撃は、メールアドレスを偽装して攻撃メールを送信する場合が多い従来のフィッシング攻撃と異なり、乗っ取られた正規のアカウントから実行されます。このため、送信者プロパティまたはメールヘッダをチェックして偽装された送信者を特定するようにユーザに指示しても、無意味です。

ユーザは、ラテラルフィッシング攻撃を検出できるように、すべてのリンクをクリックする前に慎重にチェックできる場合が多いです。すべてのメール内のリンクのテキストだけでなく、実際のリンク先をチェックすることが重要です。

2. 高度な検出技術

ラテラルフィッシング攻撃はメールベースの攻撃の高度な進化を表しています。ラテラルフィッシングメールは、正規のメールアカウントから送信されるため、トレーニングを受けた知識の多いユーザにとっても検出しにくくなっています。企業は、ユーザがフィッシングメールを手動で検出することに依存せずに、AI（人工知能）とML（機械学習）によってフィッシングメールを自動的に検出する高度な検出技術およびサービスに投資する必要があります。

3. 2FA（2要素認証）

ラテラルフィッシング攻撃のリスクを軽減するために役立つ最も重要な対策の一つはアプリ、ハードウェアトークンなどの強力な2FAを使用することです。ハードウェア以外の2FAソリューションは、フィッシングの影響を受けやすいですが、攻撃者が乗っ取ったアカウントにアクセスすることを制限および抑制するために役立ちます。

このレポートはセキュリティ調査の主要な学会の一つであるUSENIXセキュリティシンポジウムで発表されます。

Barracuda
Your journey, secured.

Datasheet 19.09版 • Copyright © バラクーダネットワークスジャパン株式会社 〒141-0031 東京都品川区西五反田8-3-16 西五反田8丁目ビル 5階
Tel 03-5436-6235 • Fax 03-5436-5128 • www.barracuda.co.jp • jpinfo@barracuda.com