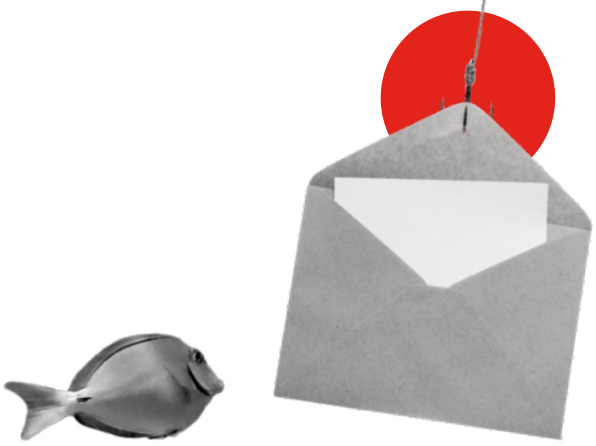
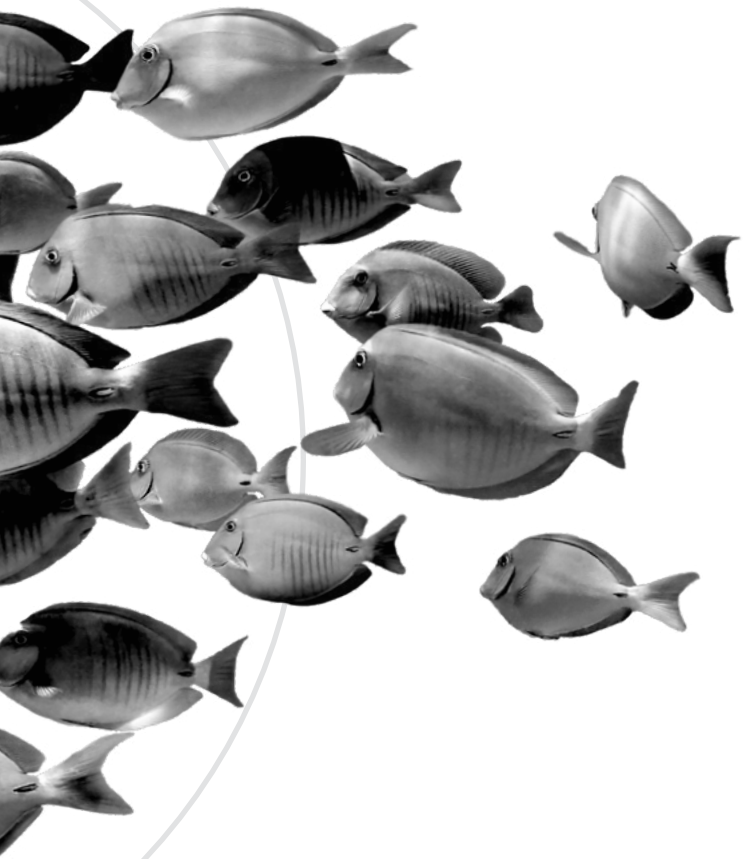
今日の脅威分析

フィッシング攻撃



Duo Security is now part of Cisco.



「

フィッシングは、攻撃者が人間性に付け込む深刻化している問題です。これらの攻撃は、攻撃を仕掛けなければ知る由もないシステムやデータへのアクセス権の取得を企てるものです。攻撃者は、ダークパターンなどの手法を用いて被害者にソーシャルエンジニアリングを行い、多くの場合金銭の獲得を目的に、盗んだクレデンシャルを活用します。企業の防御を強化するには、攻撃者からのアクセスを制限するセキュリティ制御が不可欠です。

多要素認証 (MFA) は、フィッシング攻撃者が侵害の過程で収集しうるパスワードを活用した企てを軽減するために使用できる重要な手段です。またデバイスの検証機能や適応型ポリシー適用機能があれば、攻撃者が利用できるオプションを制限できます。このアプローチをサポートする最終的な手段は、ユーザ行動分析 (UEBA) の導入です。これにより、フィッシング攻撃を防御する企業のセキュリティ担当者の状況認識が高まります」

Dave Lewis

Duo Security CISO サポート

今日の脅威分析

フィッシング攻撃

目次

巧妙化するフィッシング攻撃

クラウドサービスの使用が増加し、膨大な数のモバイルデバイスが企業アプリケーションにアクセスしているため、今日の IT セキュリティチームは、拡張された境界と攻撃対象領域の防御という困難な課題に直面しています。企業によるクラウドアプリケーションの使用が増加している上に、従業員は多くのクラウドサービスへのアクセスに複数の業務用デバイスを使用してます。

最近のリモートワークへの移行に伴い、従業員が個人所有デバイスと企業管理デバイスを仕事と娯楽の両方に使用するようになったため、これらのデバイスの境界はあいまいになっています。組織は分散する従業員に迅速に対応することを余儀なくされましたが、従来のテクノロジーに依存している中で新しいテクノロジーを短期間で導入したことにより、接続デバイスと信頼できるアクセスを中心にセキュリティ**ギャップ**[1] が生まれています。

Verizon の **2020 年データ侵害調査レポート (DBIR)**[2] によると、侵害の 67% はクレデンシャルの窃盗、エラー、ソーシャル攻撃に起因していました。この統計から、ハッカーがソーシャルエンジニアリングとスペアフィッシングに焦点を当て、疑いを持たない被害者の信頼を得てクレデンシャルを侵害していることがわかります。ハッカーがハッキングツールやフィッシングツールとその使用方法に関するドキュメントをオンラインで容易に入手できるようになったため、巧妙な攻撃はますます一般化しています。その結果、ハッカーが標的組織に侵入する際の時間とリソース面の障壁が大幅に低下し、ハッカーは組織が実施しているセキュリティ制御に関する情報を収集して、これらの制御を迂回する攻撃を実行しています。

ソーシャルエンジニアリング

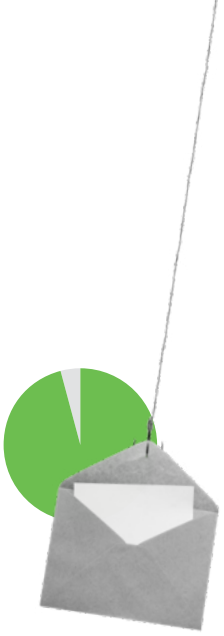
サイバーセキュリティ インフラストラクチャ セキュリティ庁（CISA）によると、**ソーシャルエンジニアリング**[3] とは、人間とのやりとり（その多くは電子メールや電話）を使用して、組織またはそのコンピュータシステムに関する情報を取得または侵害する手法です。

ソーシャルエンジニアリングでは、特定の行動を起こさせたり、機密情報を漏えいさせたりするために、人間を心理的に操作します。ソーシャルエンジニアリング攻撃者は、調査や相手を巧みに操作するやりとりで収集した情報から、組織のネットワークへの侵入や実際の従業員になりすますのに十分な情報を把握できる可能性があります。また彼らは、謙虚で礼儀正しい態度で、新しい従業員、修理担当者、または研究者であると主張したり、その身元を証明するためにクレデンシャル情報を提供することもあります。

スペアフィッシング

スペアフィッシング（標的型フィッシング）とは、標的となった個人または組織に合わせて仕立てられたソーシャルエンジニアリングの一種です。通常のフィッシングと同様に、この攻撃の目的は、機密情報の取得、マルウェアのインストール、またはクレデンシャルの窃取です。一方通常のフィッシングとは異なり、スペアフィッシングでは、個人の私的な動機、関心、インセンティブに付け込んで攻撃にだまされるように仕向けます。

このタイプの攻撃は本質的に日和見的で、組織のセキュリティの人的要素を利用します。テクノロジーに非常に精通した従業員でさえも、巧妙に仕掛けられたソーシャルエンジニアリング攻撃の被害者になることがあります。以下のケーススタディで取り上げる、注目を浴びた侵害は、まさにその状況を示しています。



96%
電子メールで送信されたソーシャルエンジニアリング攻撃の割合
（2020 DBIR）

30%
小規模企業で発生したフィッシング関連の侵害の割合
（2020 DBIR）

80%
SSL 暗号化が有効になっているフィッシング Web サイトの割合
（Statsia）

74%
HTTPS プロトコルを使用しているフィッシング Web サイトの割合
（Statsia）

ケーススタディ：

注目を浴びた最近の標的型フィッシングインシデント

概要

2020 年、ハッカーがある人気の高い企業に標的を定め、ソーシャルエンジニアリングと組織的フィッシング攻撃を仕掛けました。ハッカーは 24 時間以内に社内ネットワークにアクセスし、重要な内部システムにアクセスできるクレデンシャルを侵害し、プラットフォーム上の価値の高いユーザアカウントを乗っ取りました。

感染経路

ステップ 1

ソーシャルエンジニアリング

ハッカーは、その企業の IT ヘルプデスク担当者と名乗って複数の従業員に電話をかけ、ソーシャルエンジニアリング攻撃を実行しました。従業員に在宅勤務を許可している多くの組織と同様に、その企業はリモートアクセスに仮想プライベートネットワーク（VPN）を使用していました。また、リモートワークに切り替えてからは、VPN の問題が頻繁に発生していました。ハッカーは、被害者をだましてフィッシング Web サイトにログインさせるために、この問題を口実に使用し、報告された VPN の問題に対処しているように装いました。

ステップ 2

標的型フィッシング

問題を確認した一部の従業員は、正規の企業 Web サイトと同一に見えるクレデンシャルのフィッシング用 Web サイトに誘導されました。ハッカーは、似たような名前のドメイン上で偽のログインページをホストしていました。従業員がフィッシング Web サイトにクレデンシャルを入力すると、ハッカーはこのクレデンシャルにアクセスして、即座に正当な VPN ログインページにこの情報を入力しました。ハッカーのログインによって MFA リクエストが生成されると、一部の従業員は（偽の Web サイトへの）ログインからこのリクエストが生成されたと思い込んで自身を認証しました。その結果、ハッカーは企業ネットワークへの侵入に成功しました。

ステップ 3

ラテラルムーブメント

侵害された最初のアカウントでは、ハッカーが侵入しようとしていた重要な内部ツールにアクセスできませんでした。しかし、一度ネットワークに侵入したハッカーは、さまざまな情報システムに移動して内部プロセスの詳細を知ることができました。

ハッカーは、従業員がアクセスできる重要な内部アプリケーションやシステムへのアクセスに関する情報が含まれている内部 Web サイトを表示できました。この情報を入手したハッカーは、同じソーシャルエンジニアリングとフィッシング戦術を使用して、必要なアクセス権を持つ従業員を標的にしました。ハッカーは、重要な内部システムへのアクセス権を持つ従業員のクレデンシャルの侵害に成功し、最終的にはプラットフォーム上の価値の高いユーザアカウントを乗っ取りました。

認証のベストプラクティス

高度なフィッシング攻撃を防止

上記のケーススタディからわかるように、ハッカーはクレデンシャルを侵害し、適切なアカウントにアクセスすれば、IT チームが把握していない、インベントリに含まれていないデバイスを使用していても、組織の内部システムに侵入することができます。このような高度な攻撃を防ぐためには、ユーザ ID とユーザデバイスの信頼性を検証する、強力な認証および認可制御の導入を検討する必要があります。

ここで、高度な攻撃を阻止するのに役立つ、ID 中心のセキュリティアプローチのベストプラクティスを紹介します。

1.

多要素認証（MFA）の実装

パスワードは、ハッカーにとっては簡単に入手できるものですが、ユーザにとっては覚えるのが難しく、IT 部門にとっては保護するのが難しいものです。MFA の義務付けは、パスワードが盗まれたり侵害されたりした場合に不正アクセスのリスクを軽減できる重要なセキュリティ制御です。MFA にはいくつかのユーザ認証方式がありますが、すべての MFA 方式が同様に強力なわけではありません。MFA 認証方式として SMS またはテキストメッセージを使用する方法は、侵害に対して脆弱です。**SS7 インターセプトサービス**[4] や、**Modlishka**[5] などの容易に利用できるオンラインリソースを使用して、ワンタイムコードを簡単に傍受またはフィッシングできてしまうためです。

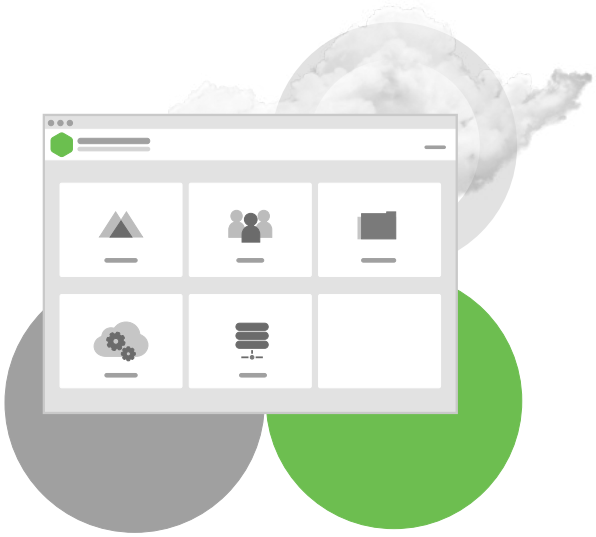
ハッカーが傍受できないモバイルの「プッシュ通知」の方が、MFA にとって安全な認証方法です。可能であれば、傍受やフィッシングが不可能な **FIDO ベース**[6]（Fast IDentity Online、強力な認証のオープン業界標準）**セキュリティキー**[7] を使用します。このキーは WebAuthn を活用し、最高レベルの認証保証を提供します。

補足のプラクティス：MFA 実装の保護

通常、MFA ソリューションは秘密キー（クレデンシャル）を使用してアプリケーションと統合し、追加の認証要素を利用します。これらの秘密キーが保護されていない場合、ハッカーは秘密キーを盗んで MFA 実装を侵害する可能性があります。秘密キーはパスワードと同様に扱う必要があります。また、重要なアクセス制御（MFA）のセキュリティと整合性を維持するために、安全に操作および保存する必要があります。侵害が発生した疑いがある場合は、秘密キーをローテーションすることをお勧めします。

2.

シングルサインオン(SSO)でパスワードへの依存を軽減

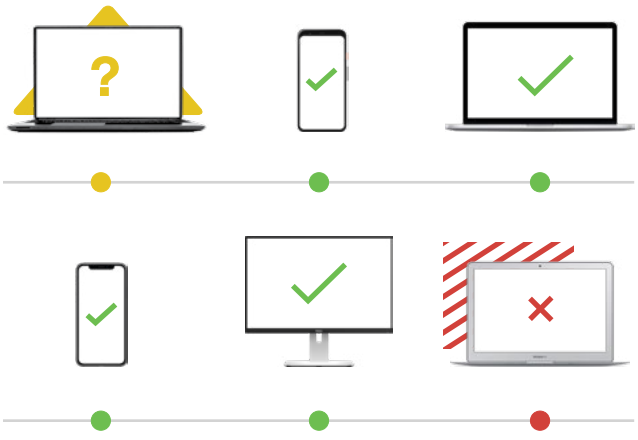


現在、平均的な企業は **1,000 を超えるクラウドアプリケーション**[9] を使用していて、通常従業員は、日常業務を遂行するために **10 を超えるアプリケーション**[10] にアクセスする必要があります。これでは人間が把握するにはパスワードが多すぎるため、パスワード疲労に陥ってしまいます。将来的に、可能な限りパスワード不要の認証オプションを提供すれば、パスワードに関連する多くの問題は軽減されます。しかし現時点では、セキュリティ侵害を発生させずにパスワード不要のプロセスを開始するには、MFA とともにシングルサインオン (SSO) を実装するのが効果的です。

SSO は、エンドユーザに対して、1 回のログインで複数のアプリケーションへのアクセスを提供します (ユーザ名とパスワードの 1 つの組み合わせを使用)。ユーザが覚えておく必要があるパスワード数を減らし、パスワードの入力回数を減らすことで、パスワードの再利用といったパスワード関連の悪い習慣をなくすことができます。管理者にとって SSO は、認証とアクセスログの統合可視化ポイント、およびリスクプロファイルに応じて各アプリケーションのセキュリティポリシーを適用する認証ワークフローの効果的なポリシー適用ポイントとして機能します。

3.

詳細なデバイスインベントリを維持



多くの組織がさまざまなレベルの個人所有デバイスの持ち込み (BYOD) を採用しています。この傾向は、最近のリモートワークの急増によって顕著になっています。BYOD により、従業員は個人所有デバイスを含む複数のデバイスを業務に使用できるようになりました。複数のデバイスとは、複数のオペレーティングシステムとバージョンが使用されることを意味します。適切なツールを使用すれば、IT チームがすべてのデバイスと関連ユーザの最新のインベントリを維持するのに役立つはずです。

4.

認証ワークフローの一部としてデバイスの信頼性を検証

認証ワークフローでは、使用されているデバイスのセキュリティステータスを考慮し、ステータスが組織で設定された要件を満たす場合にのみアクセスを許可する必要があります。主要なオペレーティングシステムには、インストールが必要な緊急セキュリティパッチが定期的に発行されます。アクセスを許可する前に更新がインストールされていることを確認することで、セキュリティをさらに強化できます。

重要な内部システムの場合は、アクセス許可を会社の管理対象デバイスに限定する必要があります。これにより、ハッカーが内部システムへのアクセスを成功させるために解消すべき障害が大きくなります。内部システムへのアクセスを管理対象デバイスのみに制限し、危険なデバイスや未知のデバイスからのアクセスを防止することで、ユーザのクレデンシャルが使用されたとしても、標的型フィッシング攻撃のリスクを大幅に軽減できます。

「ユーザの認証方法は主に 3 つあります。ユーザ名とパスワード、二要素認証、そして追跡が可能な企業支給デバイスです。ほとんどのリソースへのアクセスの認証には、これらのうち 2 つを使用する必要があります。きわめて重要なリソースへのアクセス認証には、3 つすべてを使用する必要があります」[11]

Alex Stamos 氏
サイバーセキュリティ専門家

5.

適応型アクセスポリシーの適用

アクセスの保護ではコンテキストがすべてです。アプリケーションへのアクセスを許可する前に、ユーザのロール、場所、ネットワーク、およびデバイスの信頼性を考慮して、適切なレベルのアクセスを提供できるように、可能な限り各アプリケーション向けのきめ細かいポリシーを導入します。

6.

異常なログイン活動を継続的に監視

ユーザの行動分析を活用して、新しい場所や新しいデバイスからのアクセスといった疑わしいログイン活動にフラグを付け、トリアージを行います。疑わしいログイン活動は、侵害の可能性を示していることがあります。これらのアラートは、アクセスの自動ブロックや、修復またはエスカレーション用のサービスデスクチケットの生成に使用できます。

まとめ

ソーシャルエンジニアリングとスペアフィッシングは、組織のセキュリティの人的要素を悪用することで成功を収めています。セキュリティに対する特効薬はありません。そしてサイバー攻撃はますます身近なものになっています。したがって、セキュリティに対して「侵害を前提とする」、つまりゼロトラストの考え方を採用することが大切です。クレデンシャルは侵害されることを前提とし、すべてのアクセス要求は適切なレベルのセキュリティで認証する必要があると考えるのです。IT セキュリティチームは、セキュリティテクノロジーを慎重に評価して投資する必要があります。また人的要素を最小限に抑えるための機能をユーザに与え、組織全体のセキュリティを強化するプロセスを作成する必要があります。

Duo を利用して MFA を超える新しい防御を構築

組織では、ユーザおよびデバイスの信頼の確立のために、条件付きアクセスポリシーを導入して場所やデバイスのポスチャなどのコンテキスト要因を活用することで、ソーシャルフィッシング攻撃や標的型フィッシング攻撃からの防御を実現できます。

Duo のクラウドベースのセキュリティ プラットフォームは、あらゆる場所のあらゆるユーザやデバイスからすべてのアプリケーションへのアクセスを保護します。Duo は、管理者が簡単に導入でき、ユーザが簡単に使用できるだけでなく、コスト効率が高く、他のソフトウェアとの摩擦もありません。

Duo は 6 つの重要な機能によって、ID とデバイスのリスクに対応する容易でセキュアなアクセスを実現しています。

1. 安全で柔軟な**多要素認証**[12] 方式でユーザの ID を検証します。

2. Duo の**シングルサインオン**[13] は、オンプレミスおよびクラウド両アプリケーションへの一元的なアクセスを提供する、一貫したログインエクスペリエンスを実現します。

3. **すべてのデバイスを可視化**[14] し、企業アプリケーションにアクセスするすべてのデバイスの詳細なインベントリを維持します。

4. アプリケーションへのアクセスを許可する前に、管理対象デバイスまたは管理対象外デバイスのヘルスチェックとポスチャチェックを通じて**デバイスの信頼**[15] を確立します。

5. アクセスを組織のリスク許容レベルを満たすユーザおよびデバイスに制限するために、**きめ細かいアクセスポリシー**[16] を適用します。

6. **Duo Trust Monitor**[17] または **SIEM**[18] へのエクスポートログを使用して、リスクのあるログイン動作を監視して検出し、認証が必要な新しいデバイスの登録や、予期しない場所からのログインなどの疑わしいイベントを修復します。

Duo の強力なユーザ認証 (MFA) とデバイス検証 (Device Trust) を組み合わせて使用することで、管理者は各アプリケーションのリスクプロファイルに基づいて強力なアクセス制御を実装できます。重要なツールやアプリケーションに対しては、Duo でポリシーを適用して、アクセスを**企業の管理対象デバイス**[19] のみに制限することや、セキュアなアクセスの最高レベルの保証を提供する FIDO セキュリティキーを使用した認証を義務付けることができます。これにより、侵害されたクレデンシャルの使用を防ぎ、未知のデバイスや危険なデバイスから企業アプリケーションや機密データへのアクセスをブロックできます。

適応型ポリシー[20] により、最小権限アクセスモデルの原則を簡単に採用できます。ユーザのロールや場所、使用されているネットワークなどのコンテキスト要因に基づいて、ユーザに適切なレベルのアクセス権のみを確実に付与できます。階層化されたこれらの制御があれば、ユーザのパスワードがフィッシングされたり、ユーザが認証要求を承認するように仕向けられた場合でも、高度な攻撃を防ぐことができます。

「Duo は、当社のセキュリティの考え方を実現するために必要なツールになりました。現在は、ユーザがクラウドアプリケーションでレポートをダウンロードしたのか、データを操作したのかといったことや、ユーザが安全なデバイスからその操作を実行していたこと、MFA で身元が確認されたことを確認できるようになりました」[21]

Richard Hall 氏
FinancialForce 社 IT インフラストラクチャおよび運用担当シニアディレクタ

duo.com/trial で 30 日間の無料トライアルを開始してください

参考資料

[1] 「Microsoft report shows increasing sophistication of cyber threats」[英語]、Microsoft、2020 年 9 月 29 日

[2] 「Unpacking 2020's Verizon DBIR - Human Error and Greed Collide」[英語]、Duo Security、2020 年 5 月 20 日

[3] 「Avoiding Social Engineering and Phishing Attacks」[英語]、米国サイバーセキュリティ インフラストラクチャ セキュリティ庁、2009 年 10 月 22 日

[4] 「For $500, this site promises the power to track a phone and intercept its texts」[英語]、The Verge、2017 年 7 月 13 日

[5] 「New tool automates phishing attacks that bypass 2FA」[英語]、ZDNet、2019 年 1 月 9 日

[6] 「What Is FIDO?」[英語]、FIDO Alliance

[7] 「Security Keys and Duo」[英語]、Duo Security

[8] 「WebAuthn.io」[英語]、Duo Security

[9] 「93% of Cloud Applications Aren't Enterprise-Ready」[英語]、Dark Reading、2018 年 2 月 23 日

[10] 「Information and App Overload Hurts Worker Productivity, Focus and Morale Worldwide, According to New Independent Survey」[英語]、BusinessWire、2017 年 9 月 18 日

[11] 「How Twitter Survived Its Biggest Hack—and Plans to Stop the Next One」[英語]、Wired、2020 年 9 月 24 日

[12] 「Two-Factor Authentication Methods」[英語]、Duo Security

[13] 「Single Sign-On (SSO)」[英語]、Duo Security

[14] 「Device Trust Insights」[英語]、Duo Security

[15] 「Duo's Device Trust」[英語]、Duo Security

[16] 「Duo's Adaptive Authentication Policies」[英語]、Duo Security

[17] 「Duo Trust Monitor Is Here to Make Risk Detection Easy」[英語]、Duo Security、2020 年 12 月 3 日

[18] 「Duo Log Sync: Sending Your Duo Logs to Your SIEM」[英語]、Duo Security、2020 年 6 月 23 日

[19] 「Duo Trusted Endpoints」[英語]、Duo Security、2021 年 1 月 14 日

[20] 「Policy & Control」[英語]、Duo Security、2021 年 1 月 15 日

[21] 「FinancialForce | Duo Case Study」[英語]、Duo Security