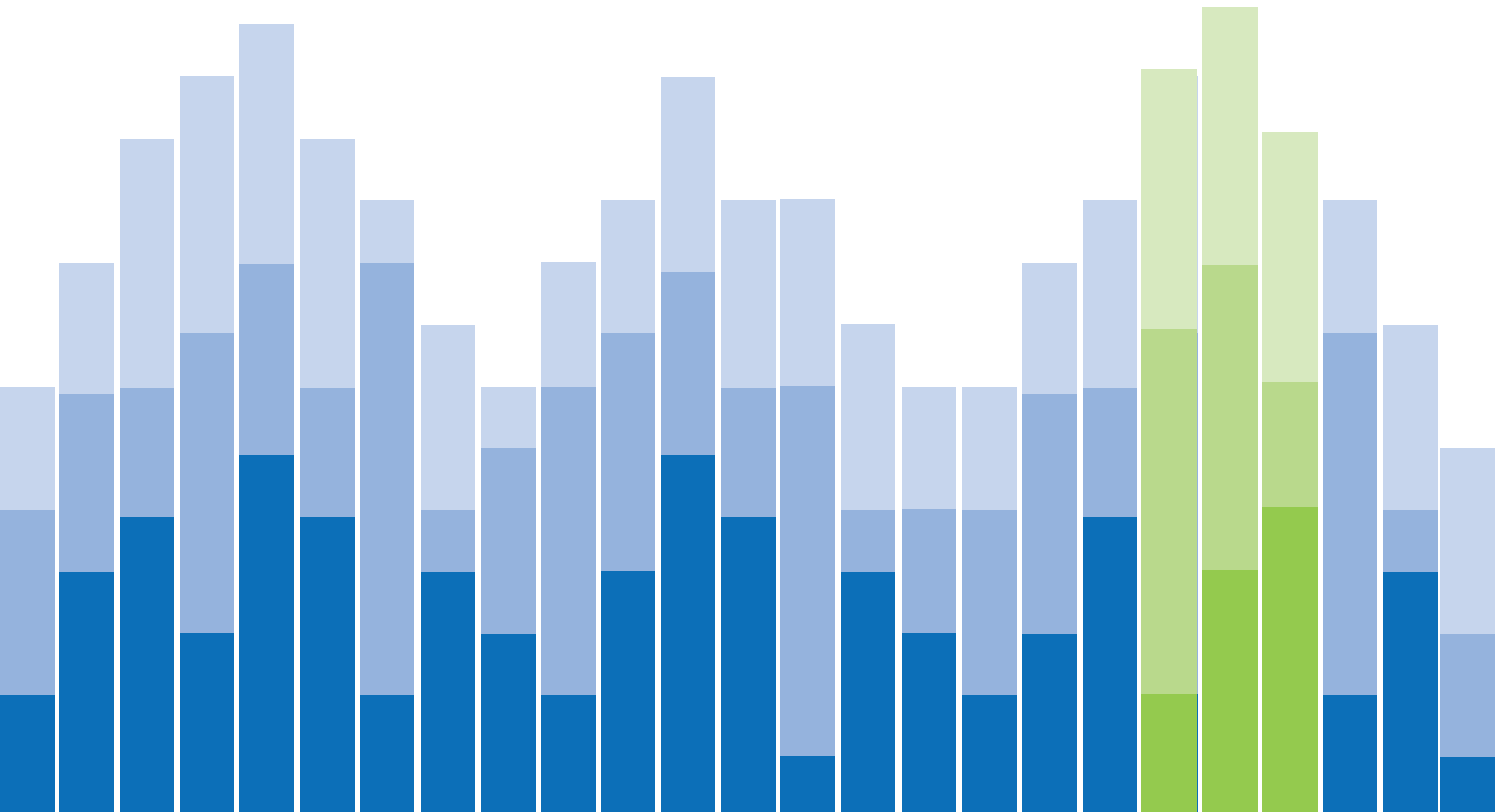
WEBROOT®
Smarter Cybersecurity™

2017 年 9 月

四半期別脅威の傾向

ますます規模を拡大し、巧妙化するフィッシング攻撃



はじめに

この数年でフィッシング攻撃の巧妙さが劇的に進化してきました。昔ながらのフィッシングの手口は大雑把に構築された大量のメールでできるだけ多くの被害者をだまそうとするものでしたが、現在の攻撃は高度な標的型になっており、この攻撃を検出し、この攻撃から逃れることは困難です。さらに重要なことは、この攻撃が蔓延していることです。

ウェブルートの最新データによると、毎月平均で 138 万 5 千もの固有のフィッシング サイトが作成されており、2017 年 5 月は驚くことに 230 万ものサイトが作成されました。大多数のフィッシング サイトは無害な活動に関連するドメインを使用してユーザーをだまします。ユーザーは正当なサイトに移動していると思い、攻撃者の成功の可能性が高まります。

フィッシング攻撃はセキュリティ侵害の第一の原因であり、世界中の組織に対する脅威としてますます増加しています。2017 年 5 月 4 日の FBI Public Service Announcement (FBI 公報)[i] によると、2013 年 10 月から 2016 年 12 月までの 3 年間に米国の企業がフィッシング詐欺のために費やしたコストは毎年約 5 億ドルに上ります。

ソーシャル メディアを使用して、個々の標的への攻撃を調整し、個人が共感する可能性のあるメッセージを使用することで、フィッシング メールの影響が大きくなりました。 経営上層部が標的となることもあります。また、Web クローラーで見つけることがきわめて難しい本物そっくりの Web ページが使用されています。被害者を巧妙にだまして、そのアカウントに侵入できる資格情報を入力させた後、その資格情報を再利用している他のアカウントにアクセスします。

本レポートでは、フィッシング攻撃を正確に検出して回避できるように、また攻撃の特性を深く理解して将来の損害を回避できるように、繰り返される最近の攻撃の傾向について詳しく説明します。本レポートに示されているデータは、ウェブルートの脅威インテリジェンス プラットフォームと BrightCloud® リアルタイム アンチフィッシング サービスで収集および分析したデータの分析に基づきます。

[i] FBI Warns of Dramatic Increase in Business E-Mail Scams (ビジネス メール詐欺の大幅な増加を FBI が警告)。 FBI Phoenix、2016 年 4 月

急増を続ける フィッシング攻撃

フィッシング攻撃は企業とエンドユーザーの両方に現在最も広まっている脅威の 1 つです。ESG の最近のレポート[ii] によると、調査の対象となった、セキュリティおよびネットワークのインフルエンサーおよび意思決定者の 63% が過去 2 年間にフィッシング攻撃を受けたと言っています。同レポートでは、回答者の 35% が今後 2 年の間にフィッシング攻撃を受けると予測し、29% がランサム攻撃を受けると予測しています。

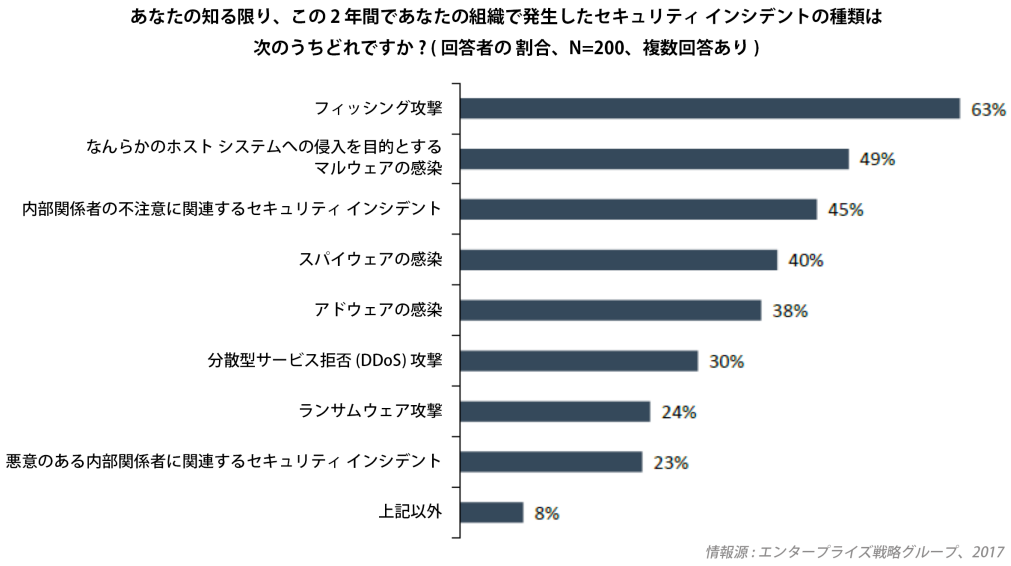


図 1: 過去 2 年間のセキュリティ インシデントの種類

[ii] 2017 Business Cybersecurity Trends, ESG Research Insights Report (2017 年ビジネス サイバーセキュリティの傾向、ESG リサーチ インサイト レポート)、2017 年、ウェブルートによる委託。

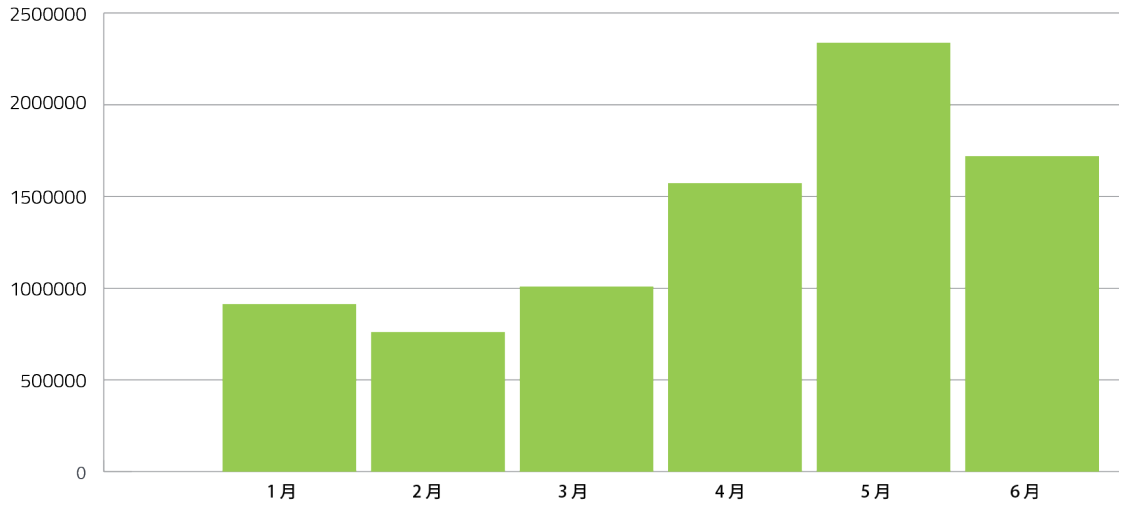


図 2: 月ごとの固有のゼロデイ フィッシング URL の件数

フィッシング攻撃はサイバーセキュリティ侵害の第一の原因です。 Verizon によると[iii]、セキュリティ侵害およびインシデントの 90% でフィッシング攻撃が確認されました。この問題の大きさは、ウェブルートのビジネス ユーザーとホーム ユーザーが 2017 年最初の 6 か月で発見した固有の (ゼロデイ) フィッシング サイトの数で示されます (図 2 を参照)。

フィッシング サイトの数は毎月平均で 138 万 5 千サイトに上ります。少ない月 (2 月) で 76 万 1 千サイト、多い月 (5 月) で 230 万サイトです。これまで、ハッカーは通常 1 つの新しいサイトを作成し、そのサイトを使用してすべての攻撃を行っていました。このため、ドメインの名前をブロック リストに入力することでそのドメインを効果的にブロックできました。現在は、不正な URL を集めてリストを作成し、その URL をブロックしようとしても、うまくいかないことは明らかです。1 時間ごとにリストが更新されたとしても、これだけの量の新しいサイトに対応することは無理です。

[iii] Verizon 2017 Data Breach Investigations Report. (Verizon の 2017 年データ侵害調査レポート)。Verizon、 2017 年。

フィッシング攻撃の巧妙さに関する傾向

これまでのフィッシング攻撃はできるだけ多くの人を標的としており、多くは 1 回の攻撃で数千または数百万人を攻撃対象としていました。このような攻撃は、十分な数の人が、感染した添付ファイルを開いたり、悪意のある Web ページへのリンクをクリックしたりすることを見込んでおり、これにより、攻撃者はマルウェアのインストールやユーザーの資格情報の収集ができるほか、機密情報を密かに抽出できました。

現在のフィッシング攻撃はこれよりはるかに巧妙になっています。2017 年最初の 6 か月のウェブルートのデータは 3 つの重要な傾向を示しています。それは、攻撃が高度な標的型であること、攻撃が高度なペイロードを備えていること、緊迫感を利用した攻撃で慎重さを欠く行動を駆り立てていることです。

高度な標的型のメール

大きな網を仕掛けて多くの被害者を一度に捕らえる旧式のフィッシング攻撃とは対照的に、現在の攻撃はスピア フィッシングを使用して、慎重に選定した個人または小規模グループを標的とします。攻撃者は LinkedIn、Facebook、Twitter などのソーシャル メディアのプロファイルを使用して、個人の好きなこと、嫌いなこと、興味のあること、心配していることを知ることができます。その後、攻撃者は個人に具体的に訴えかけるメールを作成します。このメールは受信者を対象として作成されているため、受信者は信頼できる送信者からのメッセージだと信じています。このため、標的がメールを開いてリンクや添付をクリックする可能性が非常に高くなります。

この亜種として「ホエーリング (whaling)」、つまりビジネス メール詐欺があります。これは、CEO、CFO などの経営幹部や他の意思決定者を標的とするものです。FBI によると、世界中で 22,000 を超える人がホエーリング フィッシング インシデント (ビジネス メール詐欺) を報告しています。

この調査結果は、2017 年 8 月に公開された「The 2017 Business Cybersecurity Trends report by ESG (ESG の 2017 年ビジネス サイバーセキュリティの傾向レポート)」で確認されています。境界セキュリティと境界ネットワークのインフルエンサーおよび意思決定者を対象とするこの調査では、回答者の 46% がこの 2 年間でマルウェア攻撃がより標的型になったと述べ、45% がマルウェアの数が過去 2 年よりも増大していると述べています。

高度なペイロード

フィッシング攻撃で狙われる対象が、資格情報や個人情報だけではなくなりました。現在の攻撃は、マルウェアを埋め込んでサーバーとのコマンドアンドコントロール通信をセットアップし、悪意のあるコマンドを侵害されたデバイスに送信したり、データを密かに抽出したりします。拡張されたこれらの機能によって、フィッシング攻撃が高度な脅威につながることが増えてきました。

最近の例がこの問題の範囲を示しています。2016 年、Locky ランサムウェアに感染した被害者は 400,000 人を超え、フィッシング、ランサムウェア、動きの速いワームを組み合わせた WanaCrypt0r 攻撃は世界中の数十万台のコンピューターに急速に広がりました。拡張されたこれらの機能によって、フィッシング攻撃が高度な脅威につながることが増えてきました。現在、すべてのフィッシング メールの 93% がランサムウェアにつながっています。[iv]

[iv] Kevin Lonergan, Information Age、2016 年 6 月

緊迫感

2017 年前半のウェブルートの分析では、フィッシング メールが人の恐怖や感情を刺激し、受信者が通常の予防策を講じることなく迅速な行動をとるよう駆り立てていることが示されています。メールの件名やフィッシングサイトの偽 URL で緊迫感を示唆し、不安を煽って、受信者が考える前に行動するよう促します。

通常、件名には、アカウントに対して異常な活動があったことや、最近の購入を確認する必要があること、アカウントが閉鎖される恐れがあること、緊急の請求や税金の支払いがあることなどが示唆されています。件名には「エラー」、「警告」、「アカウントの閉鎖」、「Microsoft フリー ダイヤル」、「公式な警告」などの語がよく含まれています。

このような脅しメールには、巧妙な Web ページにユーザーを誘導するリンクが記載されています。リンク先のページでは、ユーザーが早急に行動しない限り悲惨な結果になることを示唆し、不安を煽ります。攻撃の目的が資格情報や他の機密情報の開示を強制である場合も、マルウェアをエンドポイントに埋め込むことが目的である場合も、メールとフィッシング サイトの両方で切迫感を持たせてユーザーの感情を刺激し、すぐに行動するように仕向けます。下の例では、早急に行動しない場合の危険性を強調しています。ユーザーに資格情報の入力を要求するのではなく、電話で資格情報を確認することを要求しています。

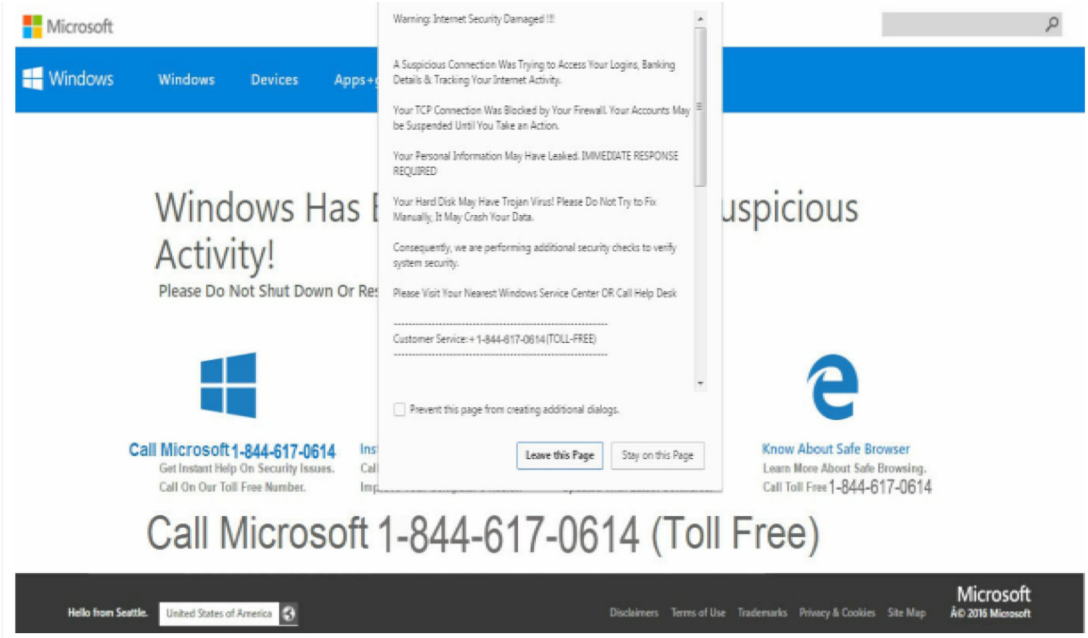


図 3: Microsoft Windows の警告通知を模倣したフィッシング ページ

検出が困難になっていくフィッシング攻撃

ウェブルートのフィッシング監視で 2017 年前半の重要な傾向が 2 つ見つかりました。それらは、フィッシング攻撃の検出をますます困難にするものです。

1. ハッカーは検出から逃れる方法を進歩させています。
2. 被害者を欺く方法がより巧妙になってきました。

検出から逃れる

攻撃が検出から逃れるための最も重要な手法は、フィッシング攻撃の短いライフサイクルと、無害なドメイン名 (PayPal、Google など) の使用です。

短いライフサイクル

2016 年、ウェブルートは、フィッシング攻撃のライフサイクルが短いことで、攻撃に関連付けられたメール メッセージや Web サイトのブロックがますます困難になってきたと報告しました。2017 年前半もこの傾向は続き、ライフサイクルは非常に短くなってきています。大半の攻撃で、オンラインになっているアクティブな時間の平均は、わずか 4 ～ 8 時間程度です。

こうしたサイトは、従来のフィッシング対策戦略 (ブロック リストなど) による検出から逃れることを目的に作成されています。活動時間が数分または数時間しかない場合、悪意のある活動が疑われる IP アドレスと URL のリストに登録される頃には活動がとっくに終わっています。1 時間ごとにリストが更新されたとしても、そのリストは一般に 3 ～ 5 日で古いものになってしまいます。あるサイトがフィッシングサイトかどうかという判断を数日ではなく数ミリ秒のうちに行う必要があります。

また、悪意のあるサイトとしてしばらくの間認識されたサイトが、数時間または数日のうちに無害に戻り、もう一度悪意のある活動を行う場合もあります。このような理由で、悪意のあるサイトの静的リストは数分で古くなるため、このリストに依存することはできません。URL が要求されるたびに URL をあらためて評価する必要があります。

無害なドメイン名

2016 年のもう 1 つの傾向は、2017 年にも引き続き厄介な影響をもたらします。大多数のフィッシング サイトが、信頼されたドメイン上のページであるかのように存在します。こうしたページはインバウンド またはアウトバウンド リンクを持たない切り離されたページです。

リンクがない場合、Web クローラーがこのページを見つけることができないため、ページは隠れたままです。ページが無害なドメイン名を使用しているため、エンド ユーザーは信頼されたサイトと通信し、信頼された当事者に個人情報を開示していると信じます。

リアルタイムの URL 検証により検出を強化

この高度な欺瞞戦略には、旧式の保護戦術に依存しない、検出と保護の優れたプロトコルが必要です。これには、不十分なドメイン クローラーや静的なフィッシング ブロック リストに依存するのではなくリアルタイムの URL 検証を実行するアンチフィッシング サービスが必要です。

リアルタイム検証には、サイトのリスクを評価し、その判定をミリ秒単位で返すことができる高度な機械学習プラットフォームが必要です。これにより、サイトが有効になっている間のサイトのスナップショットなど、補足情報が提供されます。この詳細情報は、セキュリティ チームが試みの重大度を把握し、その応答に優先度を付けるのに役立ちます。

最近の ESG 調査では、回答者の 43% が新しい脅威検出技術への投資を計画しています。これは、機械学習の進歩によって精度が向上し、誤検知が減少し、脅威の検出と修復が加速された結果と考えられます。

リアルタイム フィッシング対策のための機械学習

1. ゼロアワー攻撃に対抗するには、要求の実行時に各 Web ページを検証する必要があり、判定をミリ秒単位で配信する必要があります。これを行うための唯一の効果的な方法は、クラウドベースのインフラストラクチャを介して大規模に配信された高度な機械学習を使用することです。

2. 機械学習モデルでは、数百ものサイト属性を考慮するほか、Web および IP レピュテーション、サイトの存続期間、最近の脅威の履歴などを把握するコンテキスト分析エンジンから得られた相関するインテリジェンスを考慮しながら、高度なヒューリスティックを使用して、要求された URL を即座に評価します。

3. 入力ソースには、アクティブなスキャンとサードパーティ リストを含めることができます。重要なことは、脅威調査者とセキュリティ分析者がモデルにフィードバックを提供していることです。これが反復調整につながり、アルゴリズムと機能が時間の経過と共に向上します。

4. 機械学習ベースのフィッシング対策ソリューションはセキュリティ プロバイダに価値を即座に提供します。このソリューションは他の方法よりも 3 ～ 5 日早くフィッシング サイトを検出します。サイトが短期間のみアクティブな場合、これは不可欠です。

5. スピードと精度が非常に重要な要素の場合、機械学習はフィッシング攻撃に対して高精度のリアルタイム保護を提供するだけでなく、コンテキストに沿った脅威のインサイトを提供し、戦略インテリジェンスを促進します。

被害者を欺く

フィッシング攻撃者がエンドユーザーを欺く方法がより巧妙になってきました。2017 年前半、ウェブルートは、セキュリティに精通したユーザーさえも欺く、巧妙に作成された偽装 Web サイトと他のツールが継続的に使用されていることを確認しました。

特定が難しい偽サイト

正当なサイトを真似ようとするこれまでのページは粗雑であり容易に特定できるものでしたが、現在のページは巧妙であり、本物のように見えます。使用されている色、レイアウト、フォント、ロゴはサイトの正当なページと同じです。

こうしたサイトは、エンドユーザーまたはセキュリティの専門家でさえ、フィッシング サイトが偽サイトであるかどうかを解明することが困難です。これは、攻撃者が Web サイトの正当なページを自分の目的に合わせて修正して使用していることが多いためです。

フィッシング教育プログラムでは、ブラウザのアドレス バーを見て疑わしい URL がないかどうか確認するようユーザーに教えます。現在のフィッシング攻撃者はこれを知っているため、スクリプトを使用して無害のアドレスでユーザーを欺きます。

図 4 は、PayPal の Web サイトを偽装しているフィッシング サイトの例です。これには、不十分なドメイン クローラーや静的なフィッシング ブロック リストに依存するのではなくリアルタイムの URL 検証を実行するアンチフィッシング サービスが必要です。

リアルタイム検証には、サイトのリスクを評価し、その判定をミリ秒単位で返すことができる高度な機械学習プラットフォームが必要です。これにより、サイトが有効になっている間のサイトのスナップショットなど、補足情報が提供されます。この詳細情報は、セキュリティ チームが試みの重大度を把握し、その応答に優先度を付けるのに役立ちます。

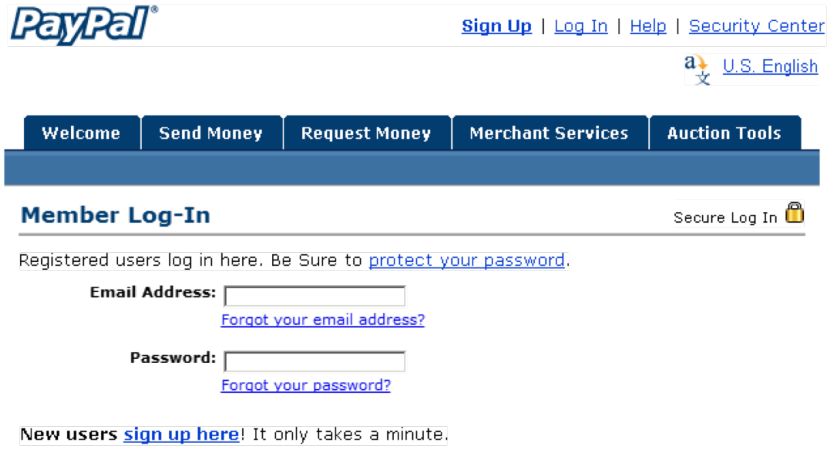


図 4: PayPal を偽装したフィッシングサイト

グラフィックスによるテキストの難読化

ウェブルートの調査で見つかったもう 1 つの手法はテキストの難読化です。上の例では、ユーザーは資格情報を快く入力しますが、ログイン フィールドのタグはグラフィックスで置き換えられています。従来のフィッシング対策の手法でこの手法を検出することは困難です。グラフィックスをテキストのようにスキャンできないため、これらのフィールドは Web クローラーから逃れることができます。

資格情報を使ってフィッシング攻撃に応答すると、そのアカウントが危険にさらされるだけでなく、同じパスワードを他の場所で使用している場合は他のアカウントへの情報ゲートウェイが作成されることがあります。

リアルタイム フィッシング対策ソリューションによる保護の強化

被害者を欺き、検出から逃れるこのような試みには、リアルタイム フィッシング対策ソリューションの即時性と精度が要求されます。巧妙な Web サイトの複製や、詐欺 URL、難読化されたテキストが、フィッシングに精通したユーザーにも対抗できない場合、機械学習に基づいてリアルタイムの URL 評価を実行するソリューションで「必要なとき」に保護を提供できます。

これは、ハッカーに匹敵する動的なアプローチです。また、エンドユーザーの生産性に影響を与えません。このリアルタイム機能は、安全な Web ブラウザとプラグインのプロバイダや検索エンジンのプロバイダが、優れた保護を顧客に提供しながらビジネスを差別化できる方法としてご活用いただけます。

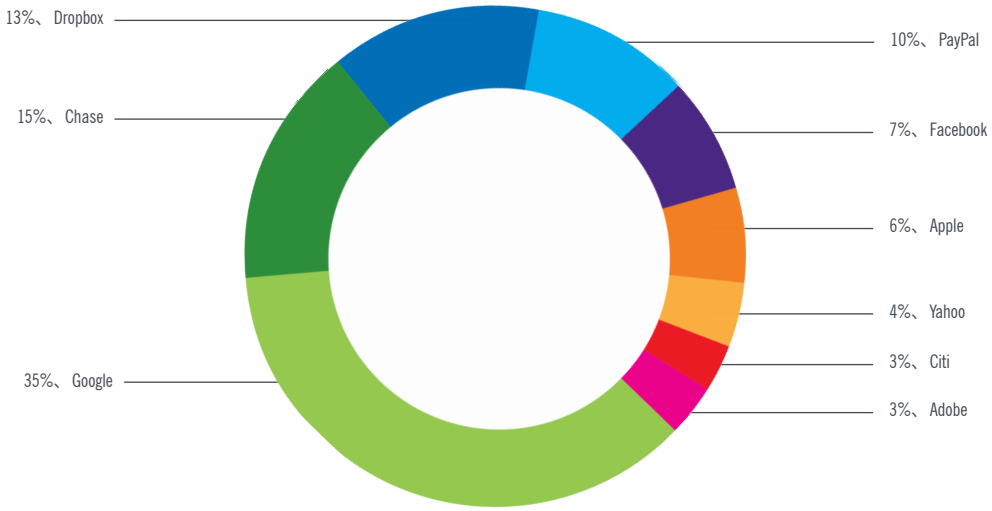


図 5: フィッシング攻撃を受けた回数が最も多い企業の上位 10 社

図 5 は、標的とされた回数が最も多い企業として Google が首位であったことを示し、その回数は、フィッシング攻撃を受けた回数が 2 番目に多いサイトである Chase (資産規模で米国最大の銀行) のほぼ 2.5 倍です。

その次に Dropbox が 13% で続き、PayPal が 10% で続きます (2017 年前半)。

2016 年のウェブルートのレポートでは、Yahoo、Apple、Wells Fargo が、偽装された回数が最も多い企業の上位 5 社に入っていましたが、今年はこれらすべての企業がその順位を大幅に下げています。今年、Yahoo は 20% から 4% に減少し、Apple は 15% から 6% に減少しました。昨年、Wells Fargo は、標的とされた回数が最も多いサイトのうちの 13% を占めていましたが、今年は 4% のみです。

金融機関を偽装するすべてのフィッシング メールに関して、標的とされた 2 つのテクノロジー企業がありました。テクノロジー企業の標的の 51% を Google が占め、19% の Dropbox がそれに続きます。

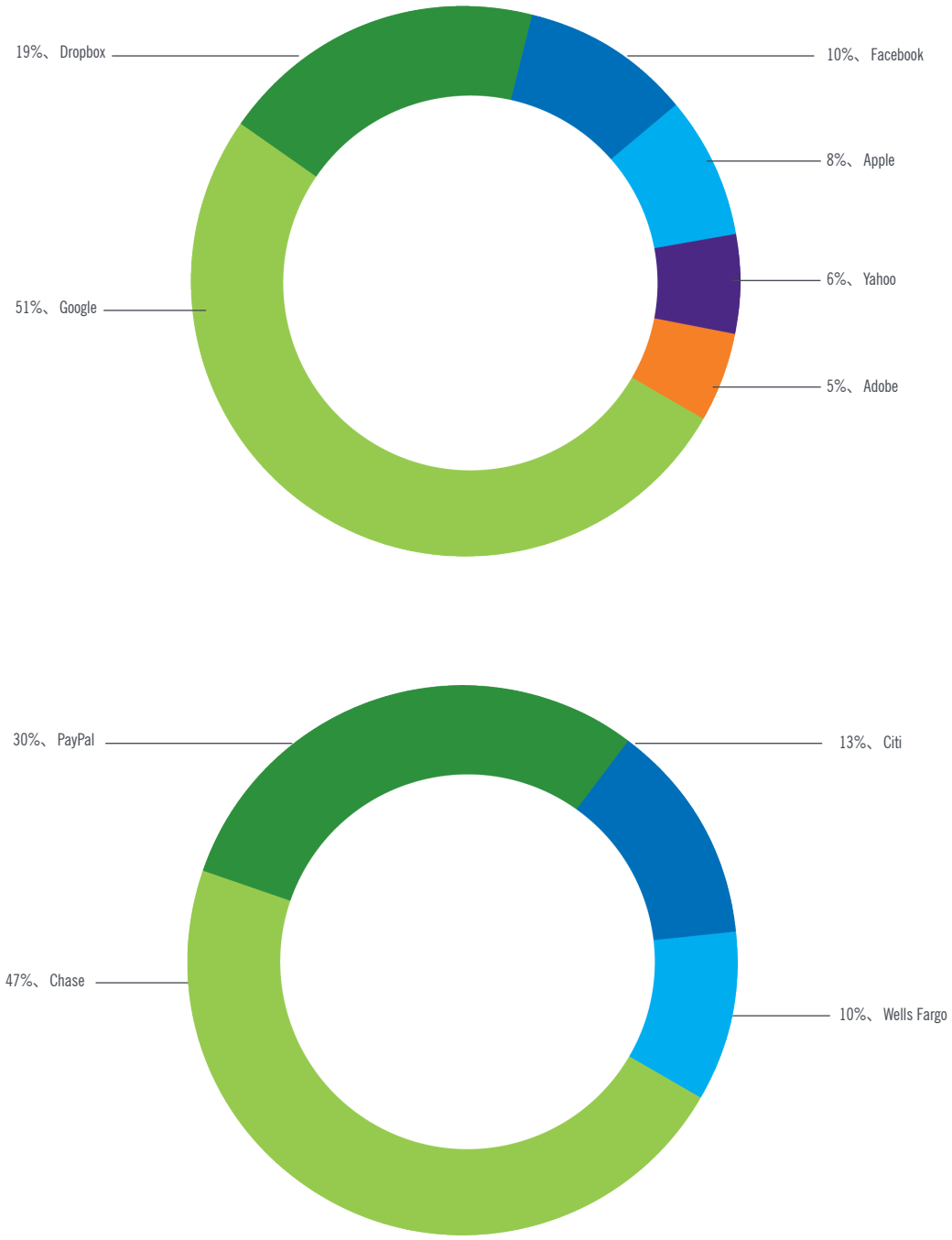


図 6: フィッシングの標的となったテクノロジー企業 (上) と金融機関 (下)

まとめ

フィッシングはなくなりません。フィッシングはこれまでになく蔓延し、巧妙になってきました。狙いすました標的設定、アドレスの難読化、現実的な偽装 Web サイトによって、フィッシング攻撃を従来の方法で検出することがますます困難になっています。このレポートで最も重要な調査結果を次に示します。

» 新しいフィッシング Web サイトが劇的に増加しました。その数は月平均で 100 万を超えます。このため、静的なブロック リストを使用してサイトをブロックすることが不可能になりました。

» 現在、フィッシング Web サイトの平均ライフサイクルは 4 ～ 8 時間です。その多くがインバウンドまたはアウトバウンド リンクを持ちません。このため、Web クローラーはこのようなサイトを見つけるのに有効な方法ではなくなりました。

» 攻撃がはるかに巧妙になり、無害なドメインの背後に隠れ、真の URL を難読化し、より悪質なペイロードを備えるようになってきました。また、現実的な偽装 Web サイトを使用して、セキュリティに精通したユーザーさえも欺くようになってきました。

» Google、Chase、Dropbox、PayPal のすべてに高い偽装リスクがあり、すべての企業はフィッシング攻撃に関連する悲惨な結果を知っておく必要があります。

危険の度合いが非常に高いため、古いフィッシング対策の手法から先に進む必要があります。脅威の最初の兆候から完全保護までの期間を最小限に抑える唯一の効果的な方法は、洗練された機械学習モデルに基づくオートメーションです。このモデルでは、各ページの要求時に要求されたページを確認することで、ページがフィッシングに関連しているかどうかの可能性を瞬時に評価できます。

このモデルは、以前に無害であったサイトは引き続き無害であるとみなすのではなく、コンテキスト情報 (最近の IP レピュテーション スコアなど) を使用してサイトの特性を相互に関連付けて判定を返します。組織はこの判定を使用して自動アクションを実行できます。検出から逃れることを目的として作成されたライフサイクルの短いサイトは、フィッシング (セキュリティ侵害の第一の原因) を回避できるほどの規模を持つ洗練された機械学習ソリューションに対抗できません。

ウェブルートについて

ウェブルートは、世界中の企業や個人を保護するためのネットワークおよびエンドポイントのセキュリティと脅威インテリジェンスサービスを提供しています。ウェブルートの高度なアプローチでは、何百万台もの実際のデバイスから得られるクラウドベースの総合的な脅威インテリジェンスを活用して、脅威をリアルタイムで阻止し、ネットワークに接続された世界のセキュリティを確保します。定評ある SecureAnywhere® エンドポイント ソリューション、BrightCloud® Threat Intelligence Services、および FlowScape® ネットワーク動作分析は、企業、ホーム ユーザー、モノのインターネットのすべてにおいて、数百万台ものデバイスを保護しています。Cisco、F5 ネットワークス、Citrix、Aruba、パロアルトネットワークス、A10 ネットワークス などの市場をリードする企業が信頼を寄せるウェブルートは、コロラド州に本社を置き、北米、欧州、アジアでグローバルに事業を展開しています。Smarter Cybersecurity™ ソリューションの詳細については、 www.webroot.com/jp/ja/ にアクセスしてください。

〒 107-0062 東京都港区南青山 3-13-18 313 南青山 8F　　電話 (米国): 800.870.8102　　webroot.com