レポート

proofpoint

THE HUMAN FACTOR 2017

www.proofpoint.co.jp

2016年のサイバー脅威を取り巻く環境の特徴は、ランサムウェアと大量のメール配信による攻撃の急増です。規模に関係なく、世界中の組織がこれらのメール攻撃の被害を受けています。これらの攻撃による直接的な被害額は数十億ドル規模に達しています。

サイバー攻撃の手法にも変化が見られ、自動化された攻撃やエクスプロイトを使った攻撃は減少し、ソーシャルエンジニアリングの手法を使い人的要因（Human Factor）を狙った攻撃が増加しています。この変化で攻撃の成功率が高まり、被害が拡大しています。メール、SaaS（Software as a Service）、ソーシャルメディア、モバイルアプリなど、サイバー犯罪者はあらゆるものを利用し、ソーシャルエンジニアリングを仕掛けてきます。特定の標的を狙う洗練された餌と広い範囲をカバーする巧妙な罠を組み合わせた、新しい強化された技術を取り入れているのです。

多くのユーザーがこの手法で騙され、マルウェアをインストールさせられたり、認証情報や重要な情報を盗まれたり、金銭を奪い取られたりしています。

目次

ソフトウェアではなく人を狙う攻撃

ソフトウェアの脆弱性を狙うのではなく、人を騙してクリックさせる攻撃が2015年から増えています。2016年はこの手法による攻撃が多発しました。12月までに、添付ファイルによる攻撃の99%は、自動化されたエクスプロイトではなくユーザーによるクリックで発生しています。URLを使った攻撃でも同様の傾向が見られ、詐欺メッセージの90%以上がユーザーを騙してフィッシング詐欺ページに誘導し、ユーザー名やパスワードなどの認証情報を入力させています。

推奨事項: 攻撃者はユーザーを騙して添付ファイルを実行させようとするため、添付ファイルに埋め込まれている悪意を持ったマクロや不正なコードを検出するソリューションを導入すべきです。URLや添付ファイルをサンドボックスでプロアクティブかつリアルタイムに検出し、分析するソリューションも必要です。リンクや添付ファイルをクリックしたときに実行される処理をサンドボックスで分析することで、従来のセキュリティソリューションでは見逃されてしまう不正な動作を検出することができます。さらに、不正なサイトかどうか特定されていない状況でも、認証情報を盗み出すWebサイトを識別できるソリューションも必要です。

調査結果のポイント

高度にパーソナライズしたメールを使い、技術的弱点では無く人の弱点を狙う標的型攻撃が増加

不特定多数ではなく、特定の個人を狙った大規模なスピアフィッシング詐欺が増加しています。これらの攻撃の多くは自動化されており、メールには標的となる受信者に関連する情報が数多く含まれています。ソーシャルエンジニアリングの手法を使う攻撃では、ユーザーを騙してマルウェアをインストールさせるために、不正なマクロやその他の手法を含む添付ファイルが使用されます。

推奨事項: 受信者に届く前に巧妙なフィッシング詐欺メッセージを検出し、ブロックできるソリューションを導入すべきです。

エクスプロイトを利用するモバイル脅威が減少し、偽のモバイルアプリや次世代型のSMSフィッシングによって銀行やコンシューマブランドの顧客を狙う攻撃が増加

攻撃者は、ユーザーを騙してモバイルデバイスにマルウェアをダウンロードさせるために、信頼されたブランドを偽装したり、紛らわしいアプリ名を使用したりするなど、様々な手口を用いています。多くのユーザーが偽のアプリとは気づかずにインストールし、個人情報を盗まれており、中にはモバイルデバイスが完全に乗っ取られるケースもあります。テキストメッセージでユーザーを騙し、ログイン情報などの重要な情報を盗み出すSMSフィッシングも増えています。ユーザーが最もよく利用し、セキュリティ対策も弱いモバイルデバイスを狙う方が、強固なセキュリティ対策を施された企業内のPCを狙うよりも効率的だからです。

推奨事項: 会社所有のデバイスだけでなく、個人所有のデバイスも保護できるモバイルセキュリティソリューションを導入すべきです。これらのソリューションは、ユーザーのクリックを検出、追跡、ブロックすることで次世代のSMSフィッシング詐欺を検出して阻止すると共に、スマートフォンやタブレットを狙った詐欺的で悪意を持った危険なアプリの存在を検知できなければなりません。同時に、金融機関、通信会社、小売業などの企業は、自社のブランドを悪用して顧客から情報を盗み出したり、不正行為を行うアプリを見つけ出すことができるソリューションを導入する必要があります。

偽のソーシャルメディアアカウントによるフィッシング詐欺が2016年に150%増加

銀行やソーシャルメディアの利用者を狙うAngler Phishing攻撃が発生しています。この攻撃では、正規のソーシャルメディアチャネルに書き込まれた顧客の投稿に偽の返信を行います。Angler Phishingは、攻撃者が信頼された企業のカスタ

攻撃者はプログラムでは無く人を利用して金銭を盗もうとするようになり、BEC攻撃がバンキング型トロイの木馬に迫る勢いで増加

メールによる金融詐欺の分野では、ビジネスメール詐欺（BEC）攻撃が急増しています。攻撃者はユーザーを騙して攻撃を行うために、不正なプログラムに頼らなくなりました。BEC攻撃は、同僚や上司になりすましてユーザーを騙し、送金や機密情報の送信を実行させようとするもので、2015年はメールによる金融詐欺全体の1%に過ぎず、バンキング型トロイの木馬よりもかなり少ない量でした。しかし2016年の終わりになると、BEC攻撃は全体の42%にまで増加しています。この増加の理由としては、大規模なサブドメインスプーフィングなどの技術革新や、標的の選択方法や送信者偽装の手口が変わったことが考えられます。

推奨事項: 攻撃の変化に合わせて、メールを動的に分類できるソリューションを導入すべきです。BECのような攻撃はメールの量も少なく、特定の個人を狙ってきます。ペイロードがない場合も多く、簡単には検出できません。隔離ポリシーとブロックポリシーを設定して、このような攻撃を阻止する必要があります。

マーサービスのアカウントになりすまし、本物のように見える投稿を行う攻撃のことです。企業のサポートを必要とするユーザーがソーシャルメディアのサポートアカウント宛てに投稿すると、攻撃者がそのスレッドに割り込み、本物そっくりのWebサイトに被害者を誘導してアカウントの認証情報を入力させます。

推奨事項: ブランドの信用と顧客を守らなければなりません。ソーシャルメディア、メール、モバイルを悪用して自社の顧客を狙う攻撃を阻止すべきですが、特にブランドになりすました偽のアカウントは悪質です。すべてのソーシャルネットワークをスキャンし、不正なアクティビティを見つけ出すことのできる堅牢なセキュリティを導入し、ソーシャルメディアを保護する必要があります。

不正なURLのクリックの半数は、企業のデスクトップ管理の対象外のデバイスで発生

不正なURLのクリックの42%はモバイルデバイスで発生しており、その数はこれまでの20%から倍増しています。また、クリックの8%は、セキュリティパッチの提供が終了している脆弱なWindowsで発生しています。

推奨事項: 従業員がどの場所でメッセージを確認しても、メールによる攻撃から保護できるソリューションを導入すべきです。スマートフォンやタブレットでの不正なURLのクリックを検出し、ブロックする必要があります。また、PCでWebサイトからメールにアクセスしたときにも、このようなクリックを阻止する必要があります。Windows PCを使用しているユーザーがいる場合には、会社所有か個人所有かに関係なく、セキュリティパッチが提供されているサポート対象のWindowsにアップグレードする必要があり、オペレーティングシステムとアプリケーションで利用可能なパッチをすべて適用する必要があります。

すべての業種にリスクが存在

すべての業種の合計でみると、不正なURLのクリック率は4.6%で、20個に１個の割合で不正なURLがクリックされていることになります。最もクリック率が高い業種は、個人情報、口座情報、医療データなどを取り扱うデジタル時代の業種ではなく、鉱業、建築業などの古い業種です。サイバー犯罪の標的に例外はありません。デジタル経済に密接に関係している企業に限らず、どの組織、業種も攻撃を受ける可能性があります。

推奨事項: 社外で働く従業員が多い企業は、金融サービス、医療機関、テクノロジ企業と同じように従業員を保護しなければなりません。最新のメール攻撃から企業全体を保護するソリューションの導入が必要です。

送信されるマルウェアの種類にも一定の傾向

マルウェアの送信時間帯は曜日によって違いはありませんが、マルウェアの種類と配信方法には大きな違いがあります。不正な添付ファイルを含むメールの多くは始業時間に届き、その4～5時間後には大幅に減少します。不正なURLを含むメールは一日の中で大きな変動はありません。攻撃者は最も効果のある時間帯を選んでメッセージを送信しています。情報を盗み出すマルウェアは週明けに多く送信されています。ランサムウェアとPoS（Point-of-Sale）を狙うトロイの木馬は週の後半に送信されています。これは、週末前はセキュリティチームが対策に十分な時間を割けないことを見越しているのです。

推奨事項: 週の後半は、自社環境内のマルウェアの監視を強化すべきです。インシデント対応を自動的に行うソリューションを導入し、数日ではなく数時間以内にセキュリティインシデントを解決する必要があります。

不正なURLのクリックの約90%は、メッセージを受信してから24時間以内に発生

メッセージを受け取ったその日が最も危険です。クリックの87%は、メッセージを受信してから24時間以内に行われており、約半数はメッセージの受信後1時間以内にクリックされています。またクリックの４分の１は、メッセージの到着後10分以内に発生しています。クリックまでの所要時間（メッセージが届いてからクリックするまでの時間）が最も短い時間帯を見ると、米国とカナダでは午前8時から午後3時の業務時間中が最も短く、所要時間は1時間未満です。この傾向は英国やヨーロッパでも同様です。

推奨事項: 被害を最小限に抑えるためには、クリックされた不正なメッセージを迅速に検出することが重要です。配信済みのメッセージにフラグを付け、配信後に不正であることが判明した場合に特定のURLのクリックをブロックできるソリューションを導入する必要があります。不正なURLが受信者のメールボックスに長くとどまるほど、クリックされる可能性が高くなります。脅威のリスクを最小限に抑えるためには、最初の24時間が特に重要になります。

ワーキングランチではなく、クリッキングランチ

攻撃者は、受信者の行動パターンを把握しています。メールの配信時間を調整し、不正なメッセージが最もクリックされやすい時間帯を狙って攻撃を仕掛けてきます。攻撃は仕事を始める頃から増え始め、4～5時間が過ぎた頃にピークに達します。そう、ランチタイムです。

この傾向は他の地域でも概ね同じで、米国、カナダ、オーストラリアではほぼ一致します。しかしフランスでは午後1時ごろにピークを迎え、スイスとドイツでは始業から1時間以内がピークになります。英国では、1日を通じでクリック数に大きな変動はなく、午後2時以降は減少していきます。

推奨事項: 不正なメッセージを読んだり、クリックしたりする場所に関係なく、ユーザーを保護するソリューションが必要です。始業時のデスクだけでなく、昼休み中のスマートフォンもモニタリングできるソリューションが必要です。

数値による解析

プログラムではなく人的要因（Human Factor）を悪用する脅威が増加

2016年の後半までに、人的要因を狙った攻撃が定着しました。金融機関を狙った詐欺メールの99%は、自動化されたエクスプロイトではなく、人を騙してクリックさせることによってマルウェアをインストールします。

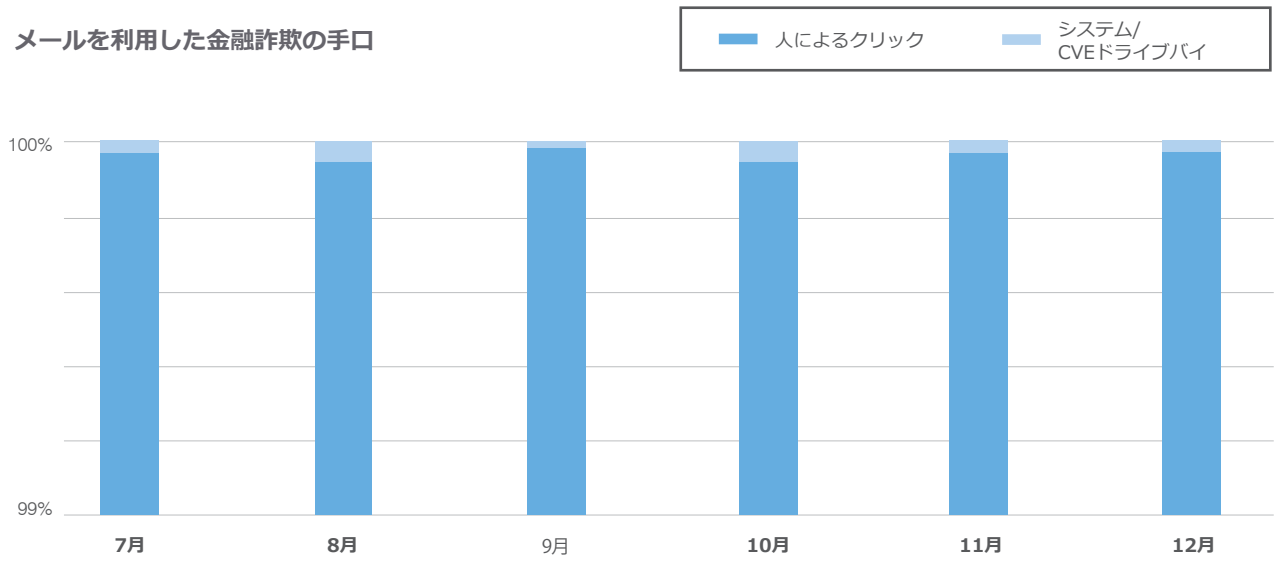


図1: メールを利用した金融詐欺で使用されたソーシャルエンジニアリングと自動化されたエクスプロイトの割合（2016年7月～12月）

この傾向は、不正なURLを利用する悪意のあるメッセージにも当てはまります。平均して不正なURLを含むメッセージの90%は、被害者をエクスプロイトキット（接続元のマシンの脆弱性を検出し、悪用するサイト）ではなく、フィッシング詐欺ページ（正式なログインページを装い、アカウントの認証情報を入力させるサイト）に誘導し、認証情報を盗み出そうとします。

人的要因を利用するエクスプロイトキット

エクスプロイトキットに比べ、自動化されたソフトウェアエクスプロイトが利用されることはほとんどありません。それでも、最近ではエクスプロイトを使って人的要因を狙う攻撃が増えています。

既に数年の稼働実績があるMagnitude EKは、エクスプロイトキット（EK）の世界で一定の評価を得ており、マルバタイジング（埋め込まれた不正なコードで正規のサイトの閲覧ユーザーを騙すオンライン広告）を収益源としています。Magnitudeは、特定の標的だけに影響が及ぶようにトラフィックをフィルタリングし、リダイレクトしています。最近では、韓国と台湾を狙ってCerberを配信しました。しかし2016年の第1四半期に、Windows 10のInternetExplorerユーザーを狙った新しいソーシャルエンジニアリングの手法を使い始めました。

この攻撃では、正規のWebサイトに埋め込まれたマルバタイジングが標的をランディングページに誘導します。このページは、ユーザーがダイアログボックスを閉じたり、迂回できないようになっており、Windowsのダイアログでよく見る一連のプロンプトが表示された後、Windows PowerShellコマンドを含むショートカットをダウンロードさせます。このコマンドがCerberランサムウェアをダウンロードし、実行します。

このソーシャルエンジニアリングを使った手法は、メールでマルウェアを配信する他の方法と本質的な違いはありませんが、攻撃の狙いが人的要因にシフトしていることは明らかです。ソーシャルエンジニアリングを利用した攻撃は、自動化されたソフトウェアエクスプロイトが持つ制約からエクスプロイトキットを開放します。その代わりにこれらの攻撃では、ユーザーを騙してボタンをクリックさせ、サンドボックスを回避してPowerShellコードを実行し、システムに侵入するためのアクションを起こします。

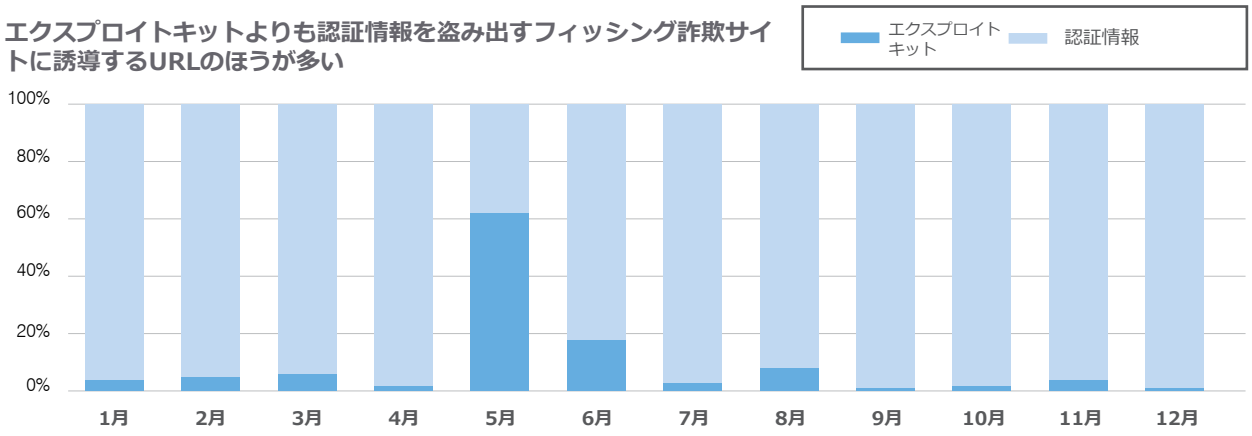


図2: 不正なURLの参照先（認証情報を盗み出すフィッシング詐欺サイトとエクスプロイトサイト）

これらの変化は、サイバー犯罪者がシステムへの感染、認証情報の窃盗、金銭の送金を行うために、自動化されたエクスプロイトではなく、人的要因を利用する攻撃手法に切り替えていることを示唆しています。

マルウェアが狙う攻撃対象

特定の地域を狙ったバンキング型トロイの木馬による攻撃も、人の弱点を利用する攻撃手法への切り替えを反映しています。これらの攻撃では、その地域の言語で作成された添付ファイルが使用され、地域に特化したWebプログラムで不正な命令を転送しています（Webインジェクション）。また、ユーザーのクリック動作の傾向に合わせて、就業時間内に攻撃を仕掛けています。

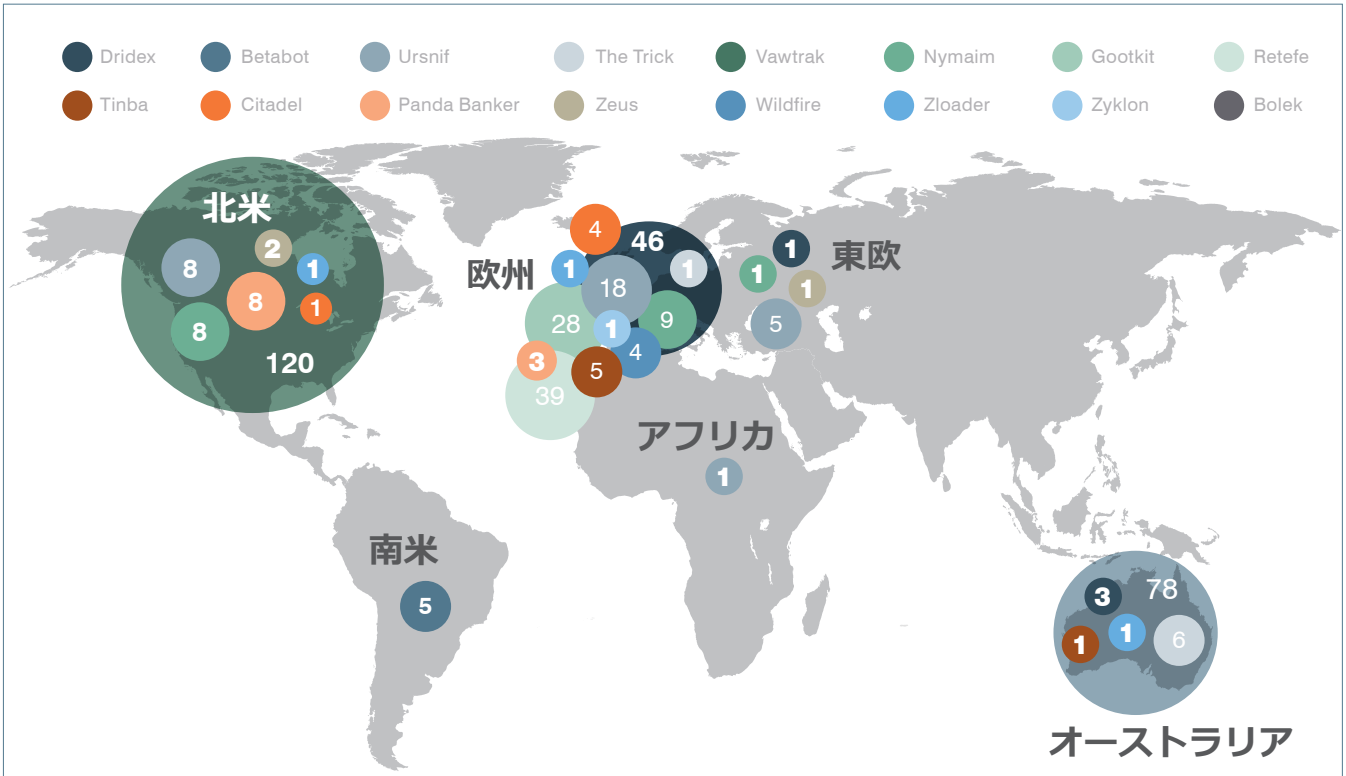


図3: バンキング型トロイの木馬の地域別活動状況（数字は攻撃の数）

推奨事項: 特定の地域を狙った標的型攻撃を検出してブロックする最先端のセキュリティ対策を導入すべきです。脅威情報を収集し、攻撃者の傾向や攻撃方法について常に最新の情報をチームで共有する必要があります。

不正なメッセージの量は曜日ごとに異なる

メールによる攻撃は毎日発生していますが、攻撃者は最大の効果を得るために、攻撃の日時を調整し、クリックされる確率が最も高い時間帯を狙ってメッセージを送信しています。多くのユーザーは始業時にメールを確認し、就業時間中にメッセージをクリックしています。

メールによる攻撃が絶える日はありませんが、日によって攻撃の量は変わります。典型的なパターンは図4のとおりです。

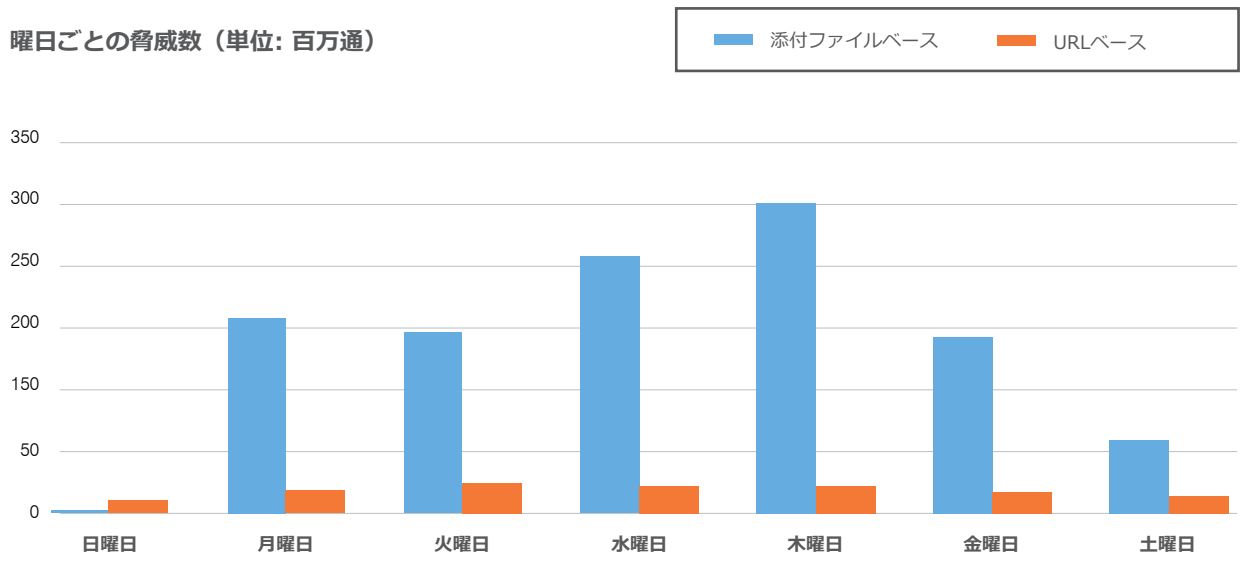


図4: 曜日ごとの脅威数

平日の平均をみると、不正なファイルが添付されたメールの量は木曜日が最も多く、平日の平均を38%超えています。これは世界的な傾向のようで、調査を実施したどの国でも木曜日の値が最も高い結果となっています。

この結果から、いくつかの重要なパターンが見えてきます。

- 平日の場合、不正なURLを含むメッセージは曜日によるばらつきが少ないという特長があります。火曜日と木曜日が比較的多く、その大半は認証情報を狙うフィッシング詐欺で使われていますが、曜日による差は過去数年と比べるとそれほど顕著ではありません。
- 週末はメールによる攻撃が少なくなります。添付ファイルの場合と比べると、不正なURLを含むメッセージの量の変化はそれほど大きくはありません。過去数年も週末のメッセージ量はごくわずかでしたが、この傾向に大きな変化はありません。

不正なURLを含むメッセージの場合、曜日別の発生量を見ると、地域ごとに差があります。調査した地域の中で、ヨーロッパは米国とカナダと異なる傾向が見られます。木曜日がピークであることは変わらず、平日の発生量の20.2%を占めています。次に多い曜日は火曜日で17.6%、月曜日、水曜日、金曜日がこれに続き、それぞれ15%を示しています。

推奨事項: あらゆるメール攻撃からユーザーを常に保護するソリューションを導入すべきです。このソリューションには、パフォーマンスや作業効率を阻害することなく、メッセージ量が最も多い日でも対応できる能力が必要です。

送信されるマルウェアの種類にも傾向がある

送信されるマルウェアの量は曜日によって異なります。また、マルウェアの種類によってそのパターンも異なります。

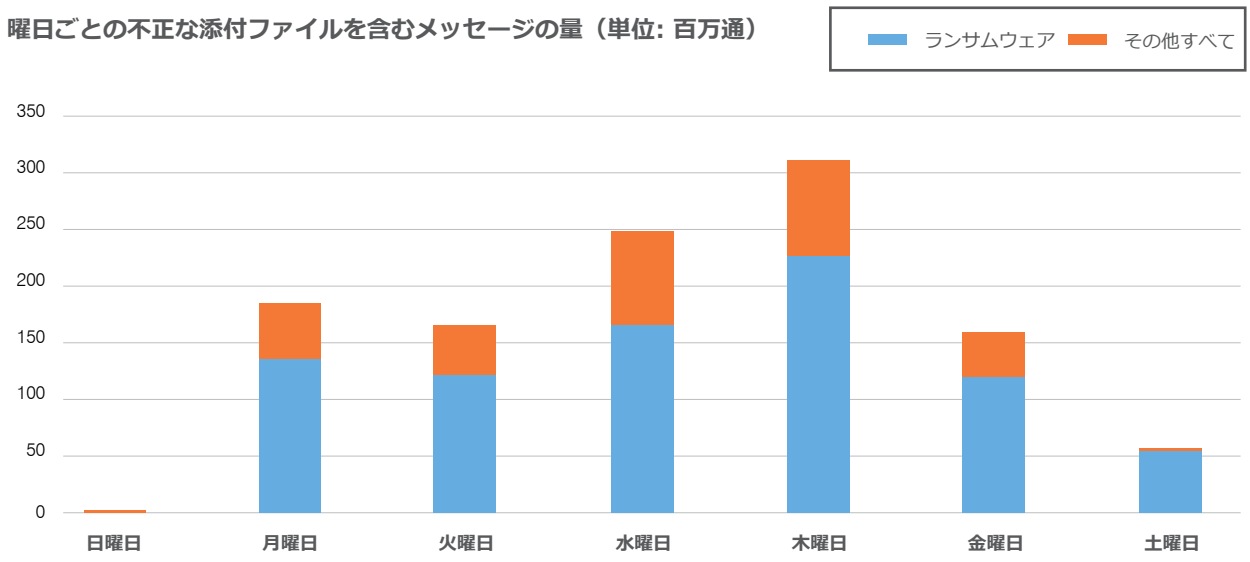


図5: 曜日ごとのマルウェアの量（種類別）

たとえば、データを人質にとるランサムウェアにも傾向があります。ランサムウェアに関連するメッセージが最も多く配信されたのは木曜日で、Lockyではこの傾向が特に顕著でした。いくつかの例外はありますが、週末に配信されるマルウェアはランサムウェアだけです。

2016年はランサムウェアが急増し、他の種類のマルウェアを凌ぐ勢いでした。図6は、ランサムウェアを除くメッセージの量を示しています。

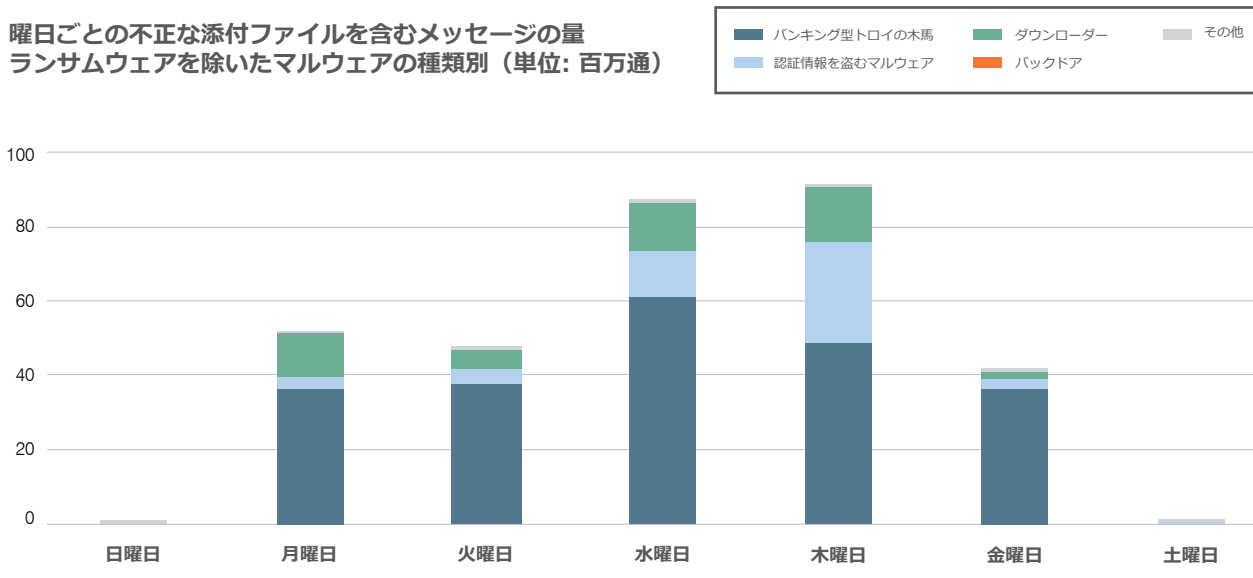


図6: 不正なメッセージの量 – マルウェアの種類別（ランサムウェアを除く）

バンキング型トロイの木馬の配信は水曜日が多く、認証情報を盗み出すマルウェアは木曜日に多発しています。ダウンローダーは月曜日から木曜日にかけてほぼ均等に配信されています。

比較的量の少ないマルウェアでは、配信日の傾向がより明確に現れます。

- キーロガーとバックドアは月曜日に多く配信されています。月曜日に配信されるバックドアの量は全体の68%で、火曜日からも木曜日までの平均を上回っています。キーロガーの場合、月曜日への偏りが顕著で、火曜日から木曜日までの平均と比べると2倍の量が送信されています。
- PoS（Point-of-sale）を攻撃するマルウェアは木曜日と金曜日に集中しています。2016年はこの2日間で80%を占めています。

非常に精巧な「餌」

フィッシング詐欺の規模と効果

フィッシング詐欺で最も使われた餌は2015年とほぼ同じです。上位5件に変動はありません。

2016年にフィッシング詐欺で使われた餌のトップ10

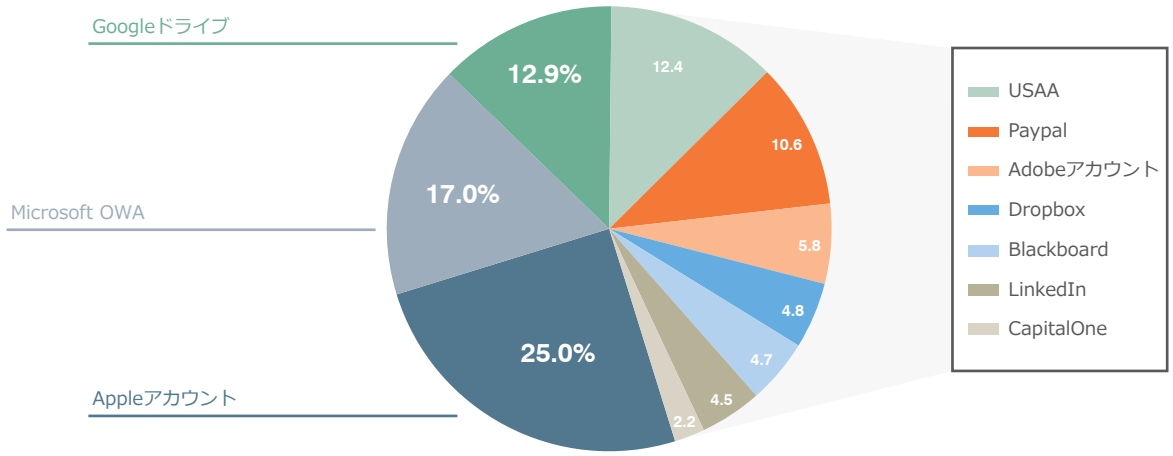


図7: フィッシング詐欺で使われた餌のトップ10

前年と同様に、2016年もメッセージの量とクリック率に相関関係はありませんでした。最も量が多かったのはApple IDを狙ったフィッシング詐欺メールですが、最も多くクリックされたのはGoogleドライブを装うリンクです。

餌として最も効果的だったのは、Googleドライブ、Adobe Creative Cloud、Dropboxなど、ファイルや画像の共有に使用するアカウントでした。これらのメッセージの量を合わせても上位10件の中で24%程度に過ぎませんが、クリック率は最も高い結果になっています。図8に示すように、メッセージの量と成功率の間には大きな差があります。

攻撃の規模と効果

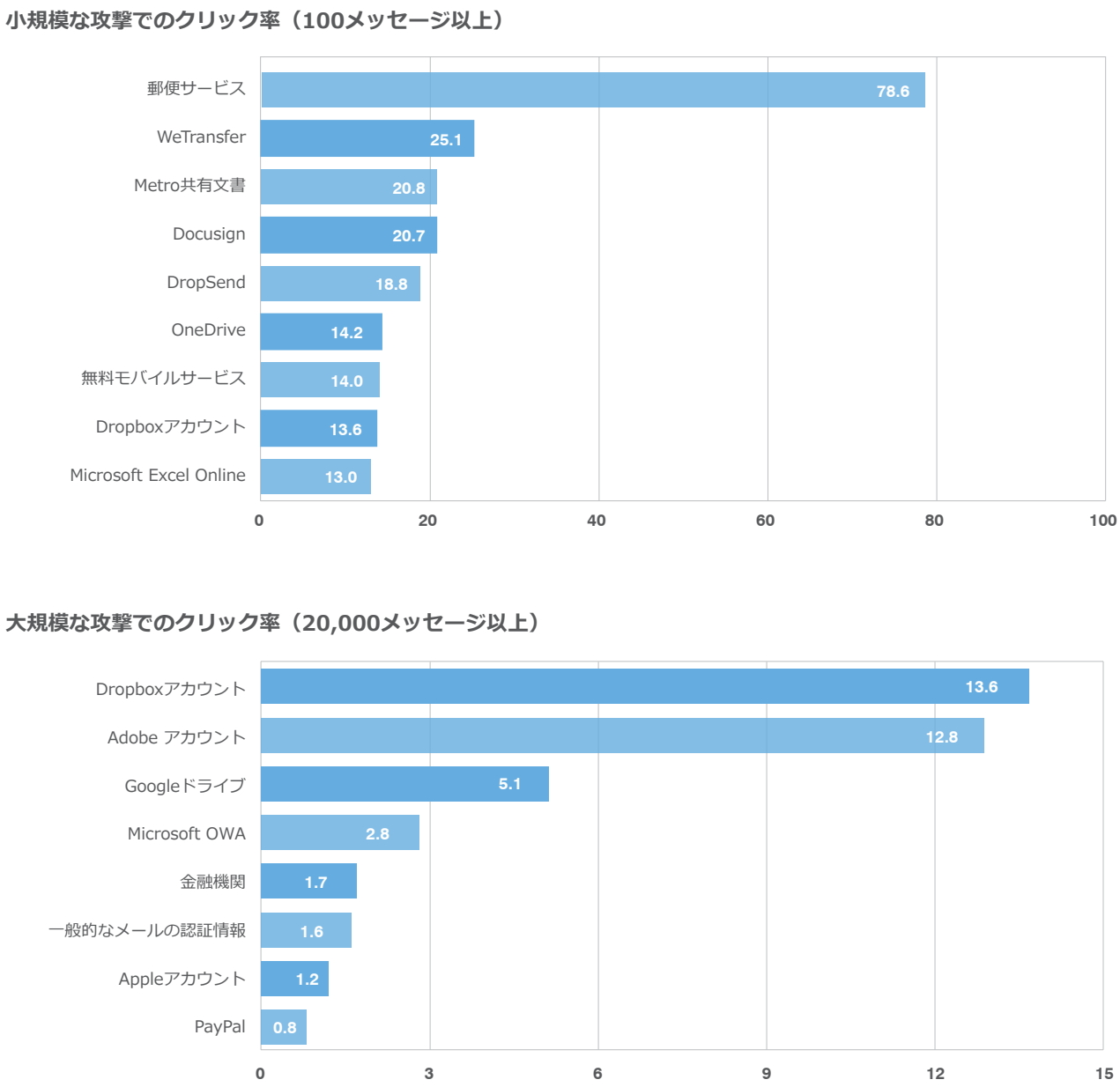


図8: よく使われる餌とクリック率（攻撃の規模別）

脅威データを見る限り、ソーシャルメディア関連の餌に大きな減少はありませんが、小規模な標的型攻撃で成果を挙げている可能性があります。一方、文書共有に対する攻撃はメッセージの量に関係なく効果的で、これを狙う攻撃者が増えています。より重要な点は、小規模な攻撃の方がクリック率が高いということです。このような攻撃を迅速に検知し、回避することは極めて重要です。

推奨事項: フィッシング詐欺の最新の餌について従業員に周知させることが重要ですが、それだけでは不十分です。餌やペイロード、送信方法などは常に変化しています。メールに含まれるURLをサンドボックスでリアルタイムに検出し、認証情報を狙う様々なフィッシング詐欺を阻止するソリューションを導入する必要があります。

クリック行動が2014年から大きく変化している

ユーザーがリンクをクリックした場所を調べると、2014年は全体の91%がMicrosoft Windows PCから実行されていましたが、この2年間でその比率は半数まで減少しています。この間、モバイルデバイスからのクリック率は倍増し、不正なURLの総クリック数の42%を占めています。

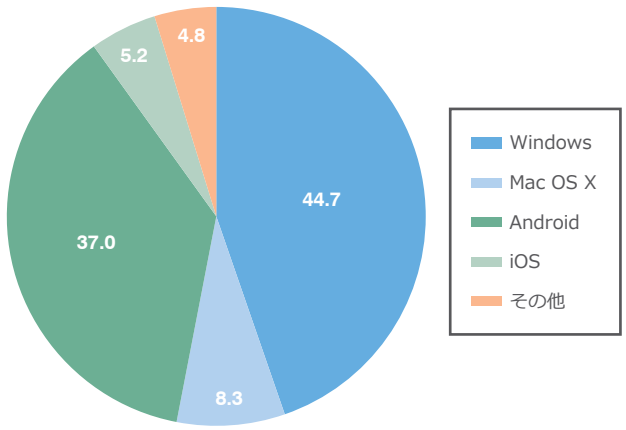


図9: クリックが実行されたオペレーティングシステム

この背景には、従業員のワークスタイルが変わり、モバイルデバイスの利用が増えたことがあります。攻撃者もこの変化を見逃さず、ソーシャルメディア、オンラインバンキングなどのモバイルアプリを使うユーザーを攻撃し、重要な情報を盗み出そうとしています。この攻撃では、自動化されたソフトウェアエクスプロイトは不要です。
次の数字からも明らかなように、セキュリティ管理者にとってWindows PCは依然として悩ましい存在です。

- Windows PCでのクリックの66%（全体の29%）は、メインストリームサポートが終了したバージョン（Windows 7）で発生しています。
- Windows PCでのクリックの19%（全体の8.5%）は、セキュリティパッチの提供が終了しているバージョン（Windows XP、Windows Vista、Windows 2000）で発生し、その数は2014年と比べると倍増しています。

自動化されたエクスプロイトで攻撃されるケースは減少していますが、メールの添付ファイルを使った攻撃で最もよく使われるエクスプロイトの一つは、4年前に見つかったMicrosoft Officeの脆弱性（CVE-2012-0158）を悪用しています。オペレーティングシステムとアプリケーションのパッチを速やかに適用しなければならないのは、このような理由によります。

業種別のクリック傾向

2016年のデータを見ると、どの企業でも不正なURLのクリックが発生しており、平均でみると、不正なURLの4.6%がクリックされています。以前と同様に業種ごとにばらつきがあり、建設業や鉱業などの古い業種のほうがデジタル時代の新しい業種よりもクリック率が高くなっています。

4.6% 不正なURLの平均クリック率（すべての業種の合計）

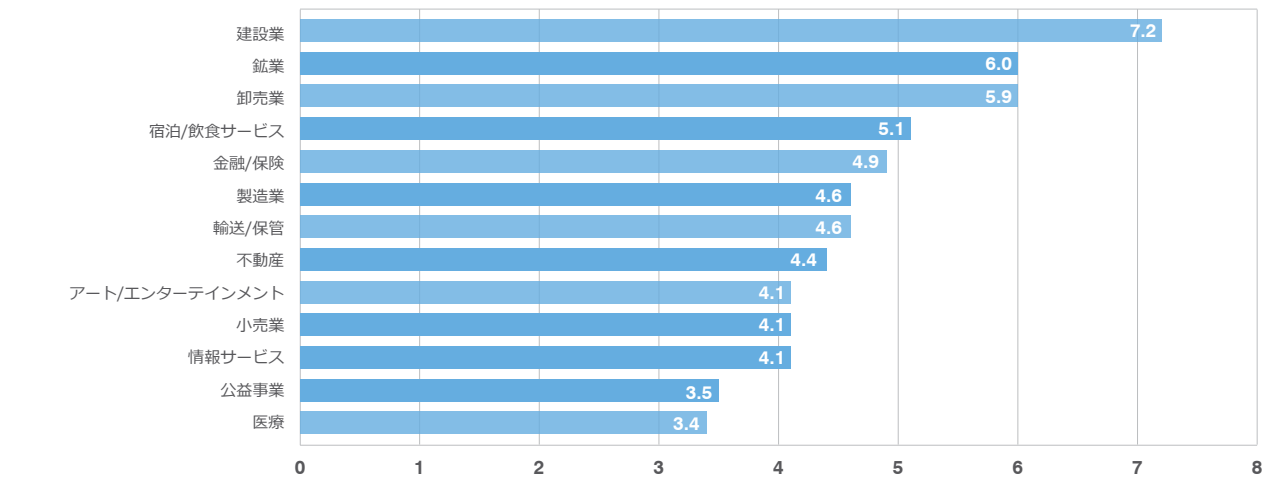


図10: 業種別のクリック率

ワーキングランチではなく、クリッキングランチ

ユーザーが不正なURLをクリックする時間帯は、どの地域でも同じ傾向が見られます。始業時に急増し、その後、4～5時間が過ぎたランチタイムの時間にピークに達します。

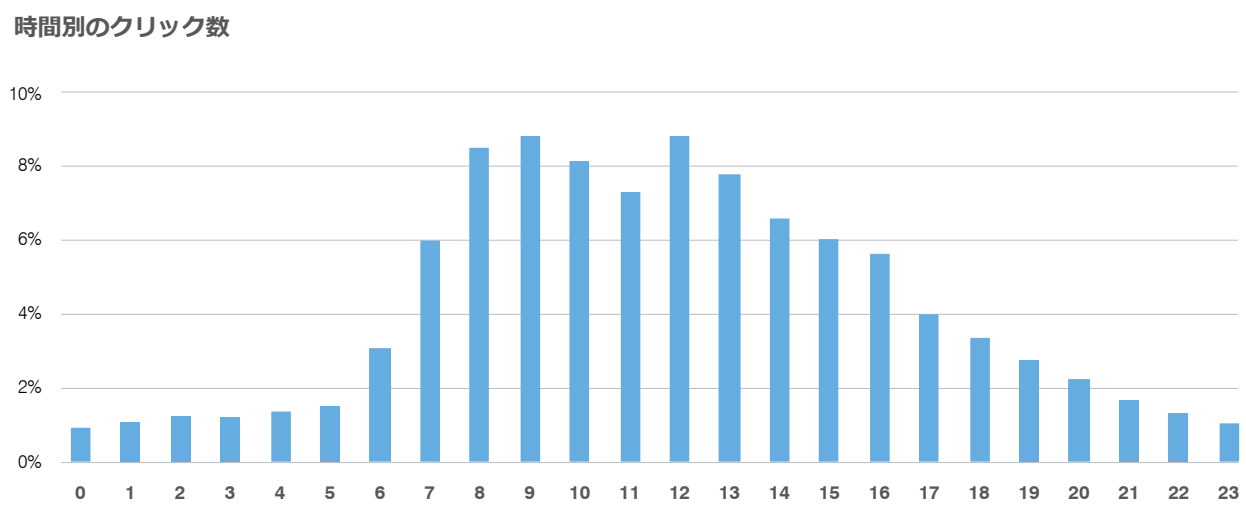


図11: 時間ごとのクリック数（すべての地域）

図11を見ると、不正なURLのクリックは一日中発生していることが分かります。職場でも自宅でも、昼夜を問わず、フィッシング詐欺ページに誘導され、マルウェアがダウンロードされています。

1日のサイクルでみると、不正なURLがクリックされる時間帯が地域ごとに異なります（図12）。

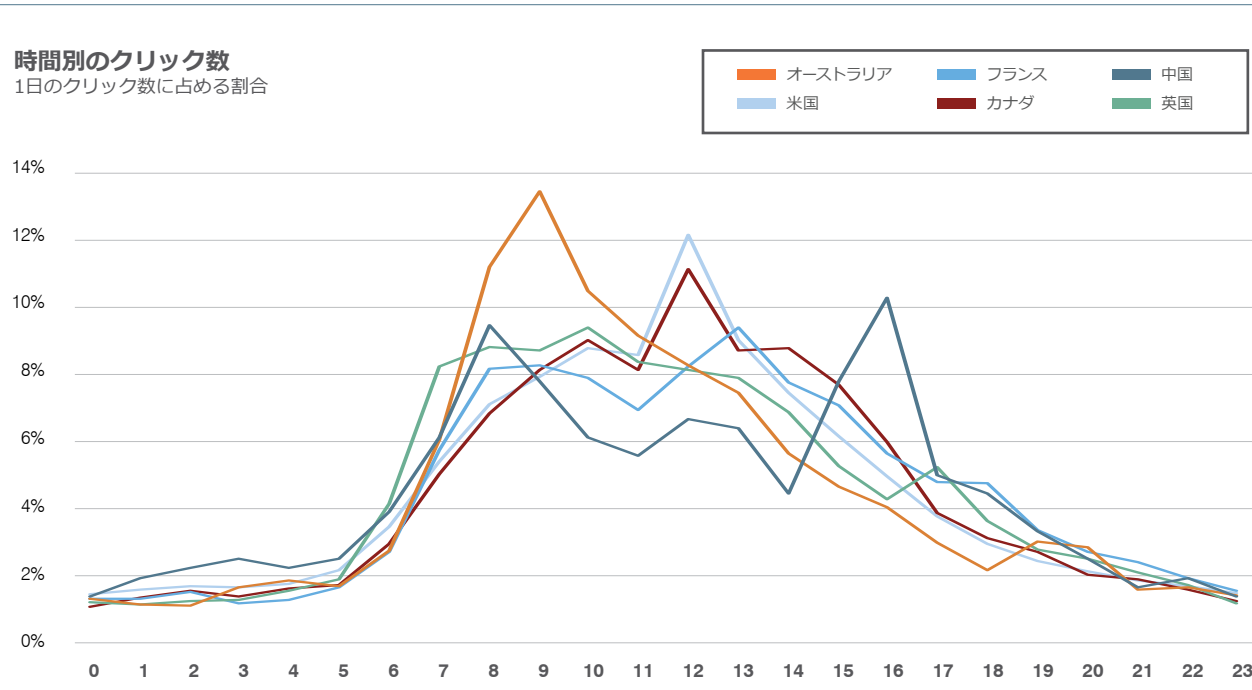


図12: 1時間あたりの不正なURLのクリック数（国別）

国別の差は次のとおりです。

- 米国、カナダ、オーストラリアでは正午がピークになります。フランスでは午後1時がピークです。
- スイスとドイツは始業から1時間までがピークになっています。
- 英国の場合、1日の中でクリック数に大きな変動はなく、午後2時以降に減少していきます。

クリックされる時間帯

ピークの時間帯は就業時間と一致しています。この時間帯は、不正なURLが短時間でクリックされており、就業時間内の場合、不正なURLがクリックまでに要する平均時間は1時間未満になります。

不正なURLの大半は、ユーザーのメールボックスに届いてから24時間以内にクリックされています。URLを送信してからクリックされるまでの時間は次のとおりです。

25.5%
10分以内に
クリックした割合

48.6%
1時間以内に
クリックした割合

87.1%
1日以内に
クリックした割合

98.3%
1週間以内に
クリックした割合

クリックまでの平均時間
（就業時間内）
1時間未満

人的要因を狙う攻撃の自動化

ビジネスメール詐欺（BEC）：人的要因を利用

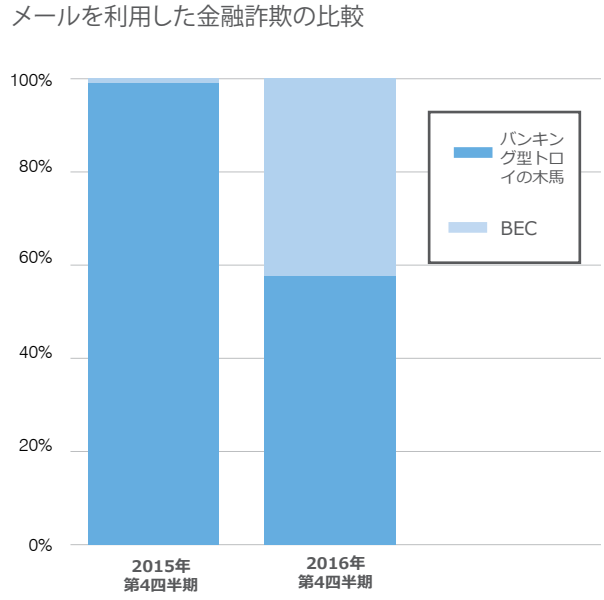


図13: 2015年第4四半期と2016年第4四半期の比較

ビジネスメール詐欺（BEC）の件数が急増し、攻撃手法も巧妙化しています。攻撃の手口は、自動化されたエクスプロイトを利用するものよりも、人に対するものにシフトしています。私達の顧客の約4分の3は、2016年の最後の3か月間にBEC攻撃を少なくとも1回以上経験しています。2015年から2016年に発生した金融機関を狙う詐欺で使用された手口を見ても、BEC攻撃はバンキング型トロイの木馬に比べ、急激に増加しています。

BECは新しい種類の脅威ですが、ユーザー側の認知の向上と自動防御技術の向上に対抗するために改良が続いています。BECの攻撃者は、CEOを装ってCFOに偽のメッセージを送信します。図14に示すように、2016年に入ると、この傾向に変化が生じます。

45%
第４四半期のBEC攻撃の増加率（前四半期との比較）

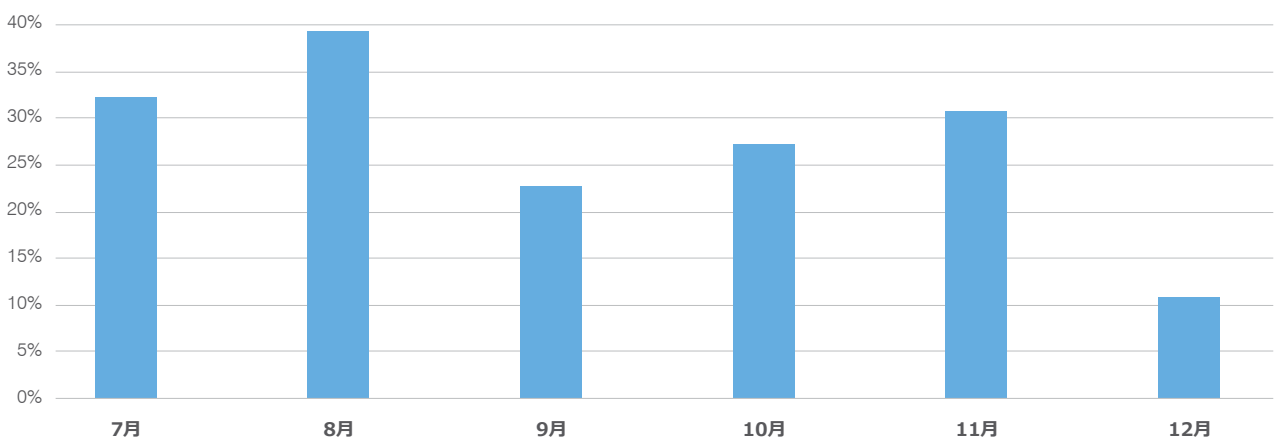


図14: CEOからCFOに送信されたBECメールの割合（2016年6月～12月）

BEC攻撃でCEOへのなりすましは引き続き行われていますが、攻撃対象に広がりが見られます。CEOとCFOの関係だけでなく、CEOと他の従業員グループの関係も狙われています。振り込み詐欺では経理部が狙われ、知的財産の窃盗では技術部門が攻撃を受ける可能性があります。また、納税記録や個人情報の収集では人事部門が狙われる可能性があります。

スピアフィッシングの大規模化：大規模なパーソナライズでソーシャルエンジニアリングを自動化

2016年以前は、メールによる攻撃を行う場合、主なアプローチは次の2つしかありませんでした。

- 不正なメールを不特定多数に大量に配信する大規模な無差別攻撃
- 巧妙な餌で特定の標的を狙う小規模な攻撃

2016年になると、これ以外の方法で攻撃を行う攻撃者が現れました。この攻撃者（私達は「TA530」と呼んでいます）は、パーソナライズされたメールを洗練されたソーシャルエンジニアリングの手法を使った大規模な標的型攻撃により配信しました。これらの攻撃では、業種別に異なるペイロードを使用し、大量のメッセージが配信されました。たとえば、小売業に対する攻撃ではPoS端末を狙うマルウェアが使用され、製造業や先進企業を狙った攻撃では、バンキング型トロイの木馬や情報を盗み出すマルウェアが使用されました。

TA530は、LinkedInなどの公開された情報源からデータを収集し、オンラインのCRMシステムからデータを盗み出し、これらの情報を使用して高度にパーソナライズされたメールと添付ファイルを餌として作成しました。これらには受信者名、役職、住所、会社名などが含まれており、それらの要素を追加することでメールの信憑性を増し、巧みなソーシャルエンジニアリングで緊急性を訴えています。

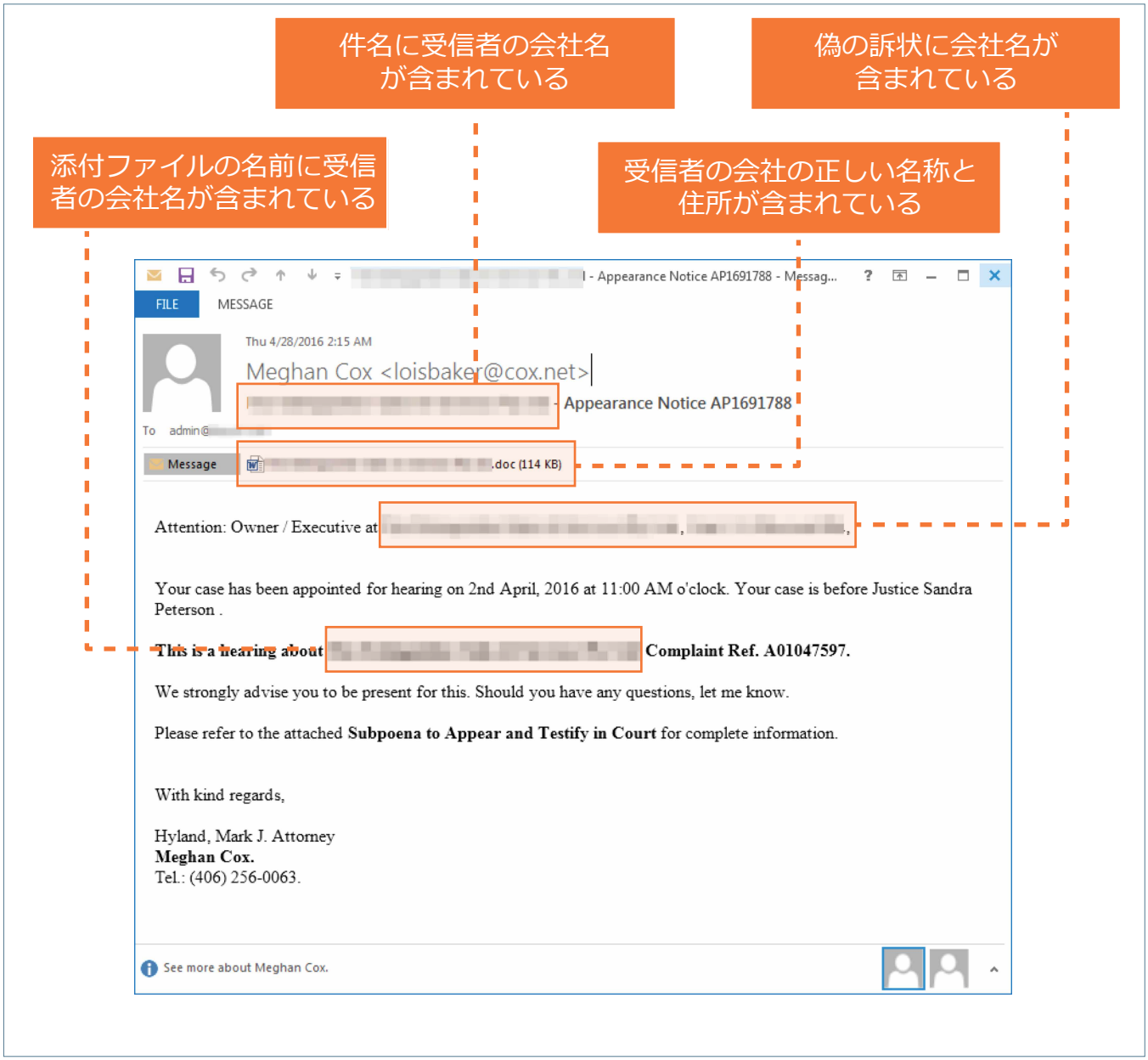
小売業に対する攻撃では、特定の店舗の住所を参照した偽のクレームを送り付けています。詳細情報が含まれているように見える文書を添付し、この問題に迅速に対応しないと訴訟を起こすと警告しています。添付文書には不正なマクロが含まれており、コンテンツを有効にするボタンをクリックすると、PoSマルウェアの亜種であるAbaddonPOSがインストールされます。

別の攻撃では、裁判の召喚状を装う文書を添付しています。ソーシャルエンジニアリングと個人情報を含むメールにより、ユーザーが添付ファイルを開く可能性が高くなります。開いた文書は召喚状のように見えますが、ソーシャルエンジニアリングの特長を持っており、文書を読むためにマクロを有効にするよう説明するイメージがオーバーレイされています。指示に従ってマクロを有効にすると、被害者のPCにUrsnifバンキング型トロイの木馬がダウンロードされます。

TA530は、他のサイバー犯罪者に様々なマルウェアを提供しています。彼らは、高度なパーソナライズと巧妙なソーシャルエンジニアリングを使い、大規模な攻撃で人的要因を狙っています。注意深いユーザーでも騙されて添付ファイルを開き、不正なコードを実行してしまうほどの巧みな手法が使われているため、多くのユーザーがバンキング型トロイの木馬や情報を盗み出すマルウェアなどの脅威に晒されています。

パーソナライズされた攻撃の構造

TA530が配信したメールは、相手の注意を惹き、メッセージの緊急性を伝えるために攻撃者がよく使う手法が使われている以外に、受信者の会社に関する情報を組み込んでパーソナライズされています。これは、手作業による小規模なスピアフィッシング攻撃では一般的な手法ですが、2016年のTA530による攻撃は、この手法を自動化された大規模なソーシャルエンジニアリングに応用しています。



モバイルを狙うソーシャルエンジニアリング

SMSを使ったフィッシング詐欺は目新しいものではありませんが、その数は急増しています。最近では攻撃の成功率を高めるため、新しい手口が使われています。メールと異なり、受信したSMSをフィルタリングする製品はまだありません。攻撃者は、SMSメッセージのほうが銀行の認証情報を入手しやすいことに気づいたのです。

42% モバイルデバイスからの不正なURLのクリック率

さらに、モバイルデバイスの画面は小さいため、サイトが本物かどうか確認しづらいことが問題に拍車をかけています。従来のSMSフィッシング詐欺では、リンクを含むテキストメッセージが使用されました。このリンクをクリックすると、通信会社などの偽のログインページに誘導されます。2016年末までには、SMSフィッシング詐欺の効率を上げるため、新しい技術や手法が利用されるようになりました。

たとえば、この時期に米国の大手銀行を装うSMSフィッシング詐欺が発生しました。これらのメッセージは複数のメールアドレスと電話番号から送信されており、本物に見えるリンクが含まれていました。

このリンク（図15、16）をクリックすると、フィッシング詐欺のフォームやサイトに移動せず、図17に示す画像が表示されます。この場合、ブランド名が画像に埋め込まれており、自動化されたツールでは解析できないため、多くのフィッシング詐欺フィルターの回避に成功しています。6秒後に被害者は本物のフィッシング詐欺サイトに自動的にリダイレクトされます。

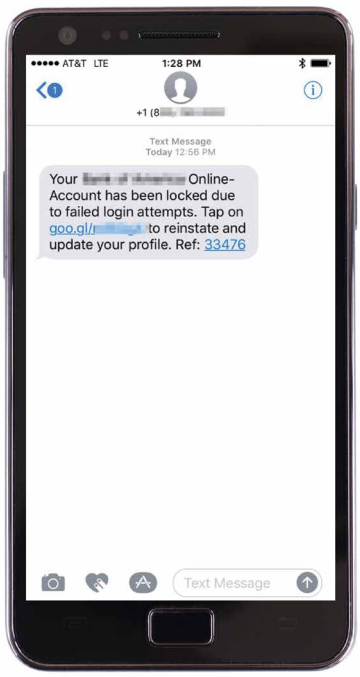


図15: 携帯電話番号で送信されたSMSフィッシング

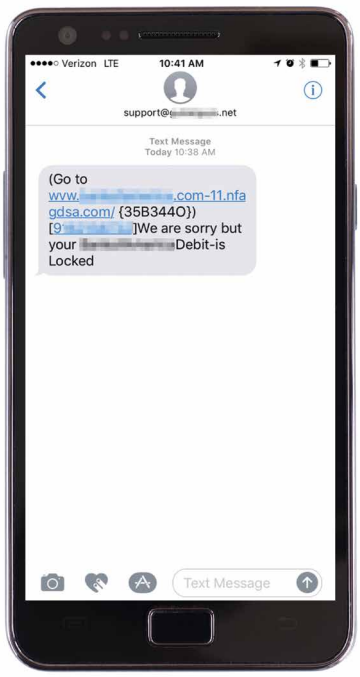


図16: メールアドレスで送信されたSMSフィッシング

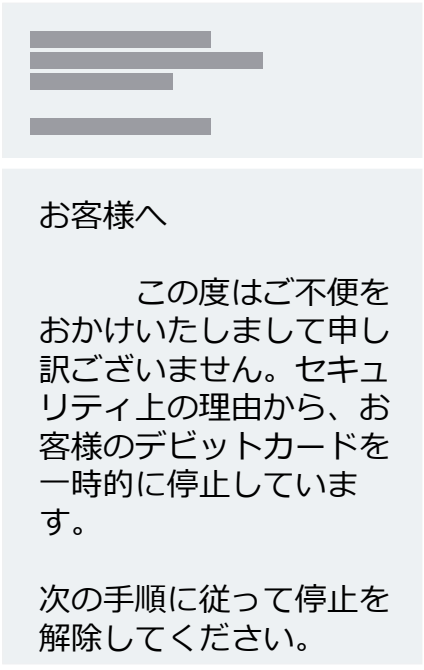


図17: フィッシングメッセージから移動して最初に表示される画像

攻撃者は3段階で検証を行います。まず、電話番号と郵便番号を確認しますが、これは「従来型」のフィッシングサイトの多くが最初にパスワードとユーザー名の入力を要求してくるのとは異なります。

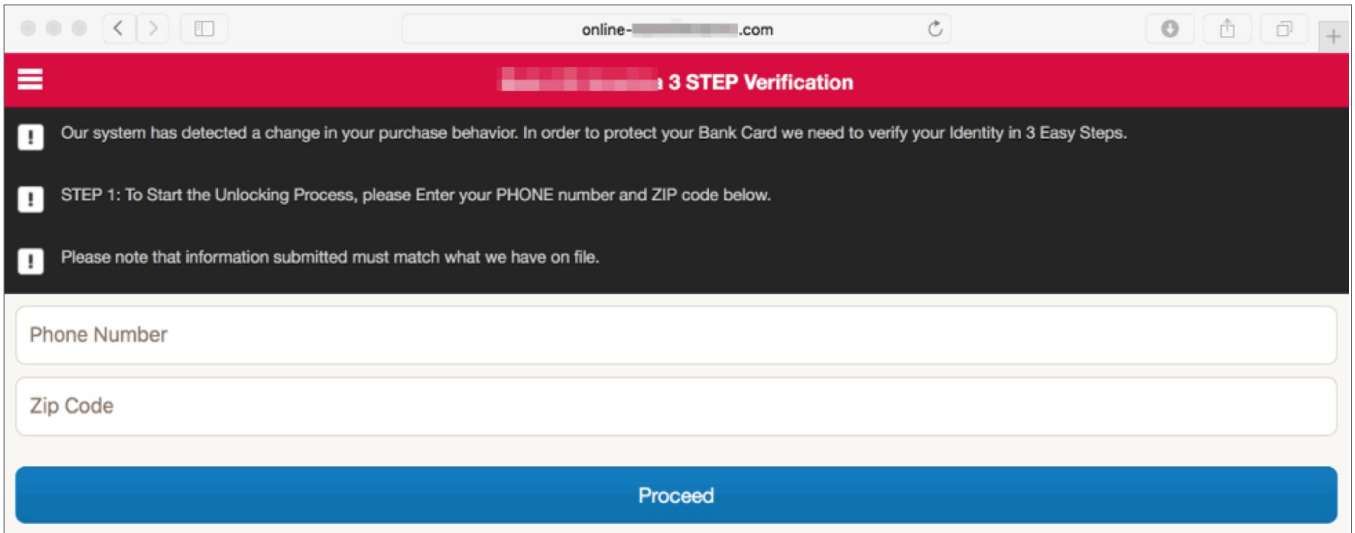


図18: 偽の確認プロセスの最初の手順。電話番号と郵便番号の入力が要求される。このリンクは編集されているが、銀行とよく似たドメイン名が使用されている。

偽の検証プロセスの次の段階で、被害者にメールアドレスの入力を指示します。受信者がGmailまたはYahoo!のアドレスを入力すると、これらのサービスの偽のログインページが表示されます。被害者がパスワードを入力すると、攻撃者はGmailまたはYahoo!のアカウントを乗っ取り、メールアドレスに紐付いたサービスのパスワードをリセットすることができるようになります。

この段階で、攻撃者は被害者の電話番号、郵便番号、メールアドレス、メールのパスワードをすでに収集しています。攻撃の最後の段階で、被害者を銀行サイトに似せたフィッシング詐欺サイトに誘導し、クレジットカード情報や社会保障番号を入力させます。この時点で受信者が不審に感じても、攻撃者はすでに携帯電話の番号を入手し、関連するメールアカウントにアクセスできる状態になっています。これだけの情報があれば、別の電話会社に乗り換え、被害者のオンラインIDを自由に操作することができます。被害者の多くはクレジットカード番号や社会保障番号も入力しているため、攻撃者はクレジットカードを不正に利用したり、個人情報を盗むことができます。

ソーシャルメディアを利用したフィッシング詐欺: キラーアプリ

2015年末以降、ソーシャルメディアのカスタマーサービスアカウントを装う詐欺が急増し、2016年には主な脅威のひとつになりました。この偽のアカウントは、人気のブランドになりすまして顧客からの問い合わせに返信するため、本物のように見えます。2016年には、このようなAngler Phishingと呼ばれる攻撃が150%増加しました。フィッシング詐欺に狙われたブランドや業種も増加しています。

例えば、Twitterを悪用した詐欺の手口は次のようなものです。John Smithというユーザーが銀行に質問をツイートします（ここでは銀行名をMajor Bank、Twitterのハンドルネームを@majorbankとします）。

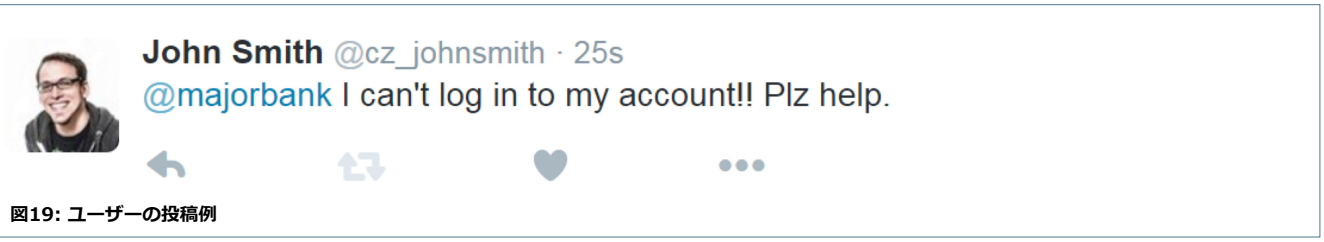


図19: ユーザーの投稿例

@majorbankとあるので、John SmithがMajor Bankの顧客で、アカウントについての問い合わせを行っていることがすぐに分かります。この情報を入手した攻撃者が会話に割り込み、John Smithに返信します。たとえば、次のような内容を送ります。

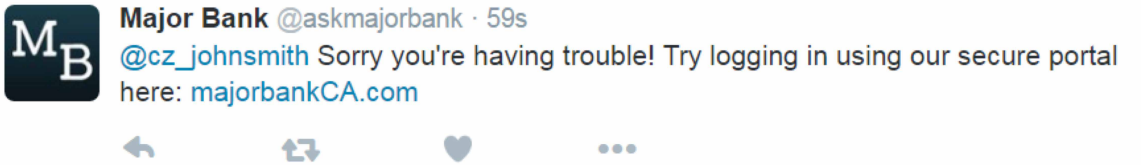


図20: Angler Phishingの攻撃者からの返信例。フィッシング詐欺のURLを送信している。

偽のアカウントは、本物に見えるようにMajor Bankのロゴとハンドル名（@askmajorbank）を使用しています。企業のサポートアカウントはメインのTwitterアカウントと異なることも多く、地域や製品に合わせて複数のアカウントを使い分けることも珍しくありません。異なるハンドル名から返信されたことに気づいたとしても、不審に思われることはありません。ソーシャルメディアの脅威はフィッシング詐欺メールよりも一般には知られていないため、大半のユーザーは攻撃に気づきません。John Smithがハンドル名の@askmajorbankをクリックすると、本物のプロフィールページに見える偽のページが開きます。

すぐに返信がきたため、John Smithは回答者が本物かどうか疑うこともなくリンクをクリックし、majorbankCA.comに誘導されます。外見上は、Major Bankのオンラインバッキングの通常のログインページに見えるため、銀行の口座番号やログインIDなどの個人情報を入力してしまい、情報が盗まれます。ここで重要な点は、John SmithもMajor Bankもアカウントが乗っ取られたことに気づいていないことです。

私達の研究者がこの種のフィッシング詐欺を最初に発見したのは2015年の終わりですが、その大半は大手銀行の顧客を標的にしていました。このような攻撃が発生したのは月に2、3回で、狙われたアカウントも少数でした。2016年の終わりまでにその頻度は増し、一部の大手銀行では毎日2、3件の攻撃が確認されました。また、攻撃対象も他業種に拡大し、オンラインバンクだけでなく、メディアやエンターテイメント業界でも被害が発生しています。このような攻撃の多くは、フィッシング詐欺用のメールアドレスとパスワード、マルウェアへのリンクを使用しています。また、別の犯罪行為で利用されることもあります。

ゲーマーを狙う

ソーシャルメディアに対する他の標的型攻撃と同様に、Angler Phishing攻撃も様々なイベントの開催日付近に集中して発生しています。たとえば、ゲーム内での賞金稼ぎを煽り、大手ゲーム会社の偽リンクをクリックさせようとするAngler Phishingアカウントが存在します。このようなアカウントは、正規のゲームやゲーム会社を装い、新しいゲームの発売に合わせて活動を活発化させています。

偽のモバイルアプリ: 外出時でも人的要因を利用

2015年から2016年の初めにかけて、人気のゲームアプリが攻撃に悪用されました。サイバー犯罪者はこれらのアプリを複製し、ユーザーに分からないように不正なコードを追加したのです。2016年末には標的が変わり、特定の銀行、特定の業種の従業員、イベントの参加者などが狙われるようになりました。攻撃者は、ユーザーを騙してモバイルデバイスにマルウェアをダウンロードさせるため、ブランドに成りすましたり、紛らわしいアプリ名を使用したり、様々な手口を用いています。

最近、中国で拡散したAndroidアプリのサンプルを分析しましたが、このアプリは大手POS端末メーカーのPoS管理アプリを装うものでした。次の図のアイコンにある中国語はメーカーを表しています。また、実際のPOSシステムの画像も表示されています。

このアプリのインストールを開始すると、デバイスへのアクセス権限が要求されますが、これはこの種のアプリには必要の無いものです。これらがどのような種類の権限であるかを見れば分かりますが、これは情報を盗み出す悪質なアプリで、バックグラウンドに常駐して継続的に実行されます。

2016年末には、なりすましアプリがiOS App Storeに現れました。このアプリは、オンラインバンキングのガイドと称し、米国の大手銀行の公式アプリの使い方やヒントを紹介しています。iOS App Storeでのアプリの説明は図のとおりです。

このアプリをインストールすると、ニュース記事と「関連アプリ」へのリンクが配信されます（図24）。このガイド自体はマルウェアではありませんが、ニュース記事からはフィッシング詐欺サイトに誘導され、さらにリンクされた関連アプリはサイドローディングされるアドウェアです。

図21: 偽のPOS管理アプリのアイコン

これは特別な例ではありません。世界中のアプリ開発者の1%以上（約16,000人のパブリッシャー）がメインストリームおよびサードパーティのアプリストアを介して不正なアプリを配布しています。ほとんどは正規のアプリを偽装していますが、実態は全く違うのです。

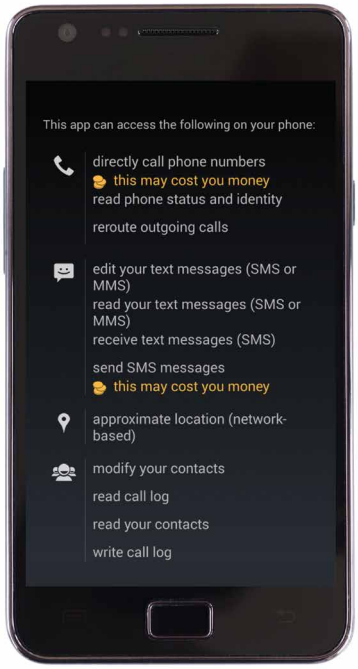


図22: 偽のPOS管理アプリが要求する権限の一部

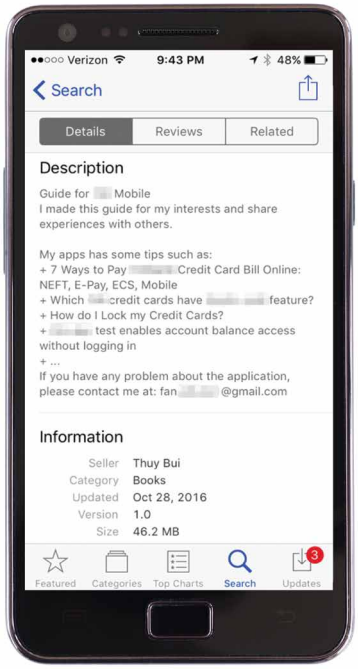


図23: iOSで表示されるモバイルバンキングガイドの説明

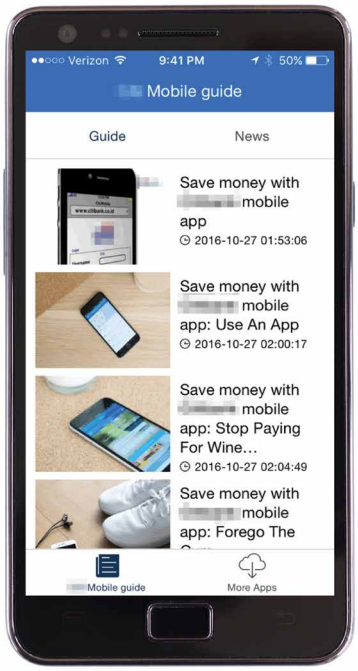


図24: このガイドアプリはアドウェアをサイドロードするための仲介役として機能し、様々なフィッシング詐欺サイトにもリンクしており、その一部はランサムウェアの配布に利用されている。

まとめ

2015年からサイバー脅威を取り巻く環境の劇的な変化が始まりました。この傾向は2016年も継続し、2017年も続くことが予測されます。不正なURLをクリックさせる攻撃でエクスプロイトキットが利用される割合は減少を続けていますが、これらのリンクの90%以上は他のサイト（認証情報を盗み出すフィッシング詐欺ページなど）に誘導するものです。また、ランサムウェアが猛威を振るい、メールを利用した新たな標的型攻撃が増加しています。ソーシャルメディアも攻撃者の武器の一つに組み込まれています。Angler Phishing 攻撃で狙われるブランドや業種が増え、この攻撃は150%も増加しています。

2016年は、モバイルデバイスなど、フィッシング詐欺で新しい攻撃経路が使用されるようになりました。今後は、アカウントの認証情報を要求するSMSやメールが増加する可能性があります。従業員がSMSに含まれる不正なリンクをクリックする割合は、これまで20%を維持してきましたが、2016年は42%に増加しました。

2016年も人的要因を狙う攻撃が多発しました。攻撃者はパーソナライズしたメールを自動的に生成し、メッセージの配信量を増やし、クリック率を高めています。サイバー犯罪者は、B2Bのマーケッターの参考書からマーケティングのベストプラクティスを学び、クリック率の最も高い火曜日と木曜日に攻撃メールを配信しています。BECと認証情報を狙うフィッシング詐欺は人の弱点を直接突いてきます。技術的なエクスプロイトは必要ありません。代わりに、ソーシャルエンジニアリングで被害者を騙し、金銭、機密情報、アカウントの認証情報を送信させようとします。

タイミングも重要です。巧妙に細工したメールを適切な時間に送信することで、攻撃の成功率が上がることを攻撃者はよく知っています。この条件は地域によって異なるため、グローバルなセキュリティオペレーションを担当している場合には、攻撃パターンだけでなく、従業員がクリックする時間や場所の傾向を把握しておく必要があります。

推奨事項

メールは組織への侵入で最も利用される攻撃経路です。このメールを保護するため、万全なセキュリティ対策を実施すべきです。従業員のメールボックスにメールが届く前に攻撃を阻止する保護対策を導入する必要があります。

挙動、プログラム、プロトコルを検証する脅威分析サービスを使用して、添付ファイルやURLに潜む脅威を検出すべきです。攻撃を初期の段階で検出できれば、防御、封じ込め、修復が簡単になります。

組織の要件に合わせて拡張できるように、クラウドベースのサンドボックス分析サービスを利用すべきです。攻撃を特定して新しいツール、手口、標的を分析できれば、次の攻撃の検知が容易になります。

社内にある会社所有のPCと同等のセキュリティで、従業員が所有するモバイルデバイスを保護すべきです。社外で働く従業員が不正なリンクをクリックする可能性が増えており、新しい攻撃経路としてSMSが利用されています。ネットワークとの接続状況や場所に関係なく、スマートフォンやタブレットでの不正なURLのクリックを検出し、ブロックするソリューションを導入する必要があります。

ブランドを悪用するAngler Phishing攻撃や、不正なアプリを阻止すべきです。ソーシャルメディアやアプリストアで会社になりすます偽のアカウントとアプリケーションをスキャンし、検出するソリューションを導入する必要があります。

また、インシデント対応の時間を短縮する必要があります。ユーザーのメールボックスに届いた不正なメールを排除するソリューションが必要です。不正なメールを除外するだけでなく、転送されるメッセージのコピーを検出して削除する機能も必要です。

PROOFPOINTについて
Proofpoint, Inc.（NASDAQ:PFPT）は、高度な脅威やコンプライアンス違反のリスクからビジネスを保護する次世代のサイバーセキュリティ企業です。Proofpointは、メール、モバイルアプリ、ソーシャルメディア経由で自社のユーザーを狙う高度な標的型攻撃を阻止し、社内の機密情報を保護できるようにサイバーセキュリティの担当者をサポートします。また、問題が発生した場合に迅速に対応できるように、適切な情報とツールを提供します。Proofpointのソリューションは、Fortune 100企業の半数以上を含む様々な規模の企業で採用されています。モバイル、ソーシャルを利用した現在のIT環境に対応し、クラウドとビッグデータを駆使した分析で高度な脅威を阻止しています。

proofpoint

www.proofpoint.co.jp