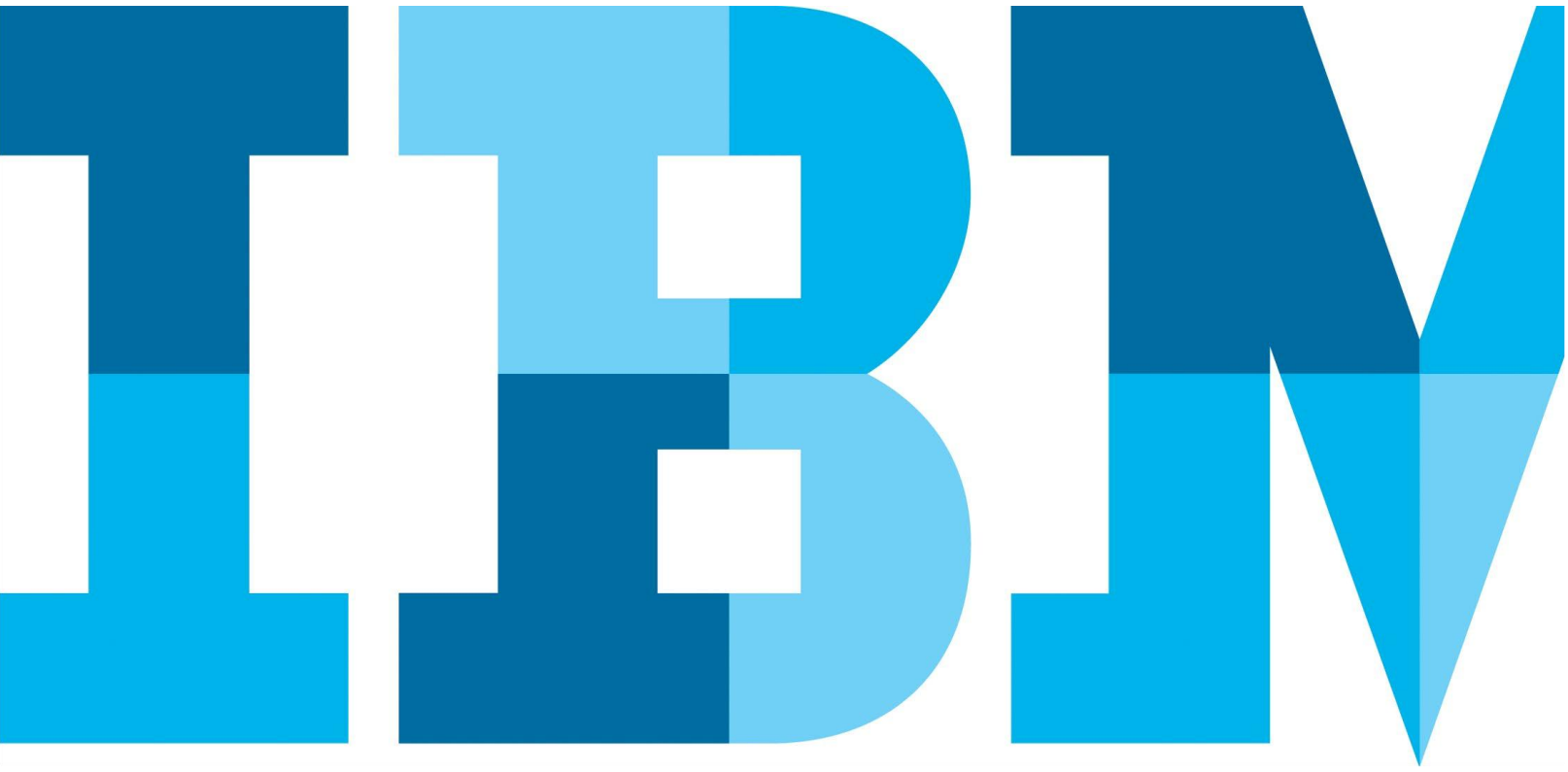
Security

Thought Leadershipホワイトペーパー

2017 年 3 月

フィッシングの検出・保護のアプローチに改革を



IBM

目次

はじめに

新しいフィッシング・サイトがオンライン・バンキングの顧客を狙って次から次へと現れます。フィッシング・ページにアクセスしたエンドユーザーの多くは、ログイン情報やクレジット・カード情報が漏えいし、詐欺犯罪者によるオンライン詐欺とクロスチャネル詐欺の両方の手助けをしているなどとは気づきません。

事実、フィッシング詐欺の成功率は非常に高くなっています。フィッシング攻撃が始まってから最初の人が犠牲者になるまでの時間は 82 秒ほどしかかかりません[1]。PhishMe の調査によると、人々はさまざまな理由、好奇心、恐れ、緊急性などでフィッシング・リンクにクリックしています[2]。

詐欺犯罪者はフィッシング・サイトが検知されてからブロックされるのは時間の問題だということを知っているので、攻撃の期間は短くなりました。通常、フィッシング・サイトが有効なのは平均 15 時間で、その間不正なキャンペーンの効率性と効果をアピールします[3]。

しかも、詐欺犯罪者は自分たちのサイトがどのように検知されるのかを把握するため、市場に常に目を光らせており、フィッシング検知を完全に潜り抜けられるように戦術を素早く変えます。

その結果、2016 年には、毎月平均 4 万以上のフィッシング・サイトが現れ、毎日 13,000 以上の新しいフィッシング・サイトが出現しています[4]。平均 85 パーセントの組織がフィッシング攻撃を受けており、その多くが非常に高度で、ターゲットに応じてパーソナライズされていました[5]。

貴行がほとんどの金融組織と同じような状態であれば、エンドユーザーがフィッシング・サイトにアクセスするのを止めるための簡単な方法はなく、組織に対するフィッシング攻撃の増加に合わせて対処する簡単な方法もないとお考えかもしれません。

しかし、それが可能になりました。

フィッシング攻撃による金融詐欺を防ぐ効果的な手立てはあるのでしょうか？

答えは、エンドユーザーが最も危険にさらされているとき、つまり個人情報や決済カード・データを開示しているときに守ることができるかどうかにかかっています。

このホワイトペーパーでは、フィッシング戦術が進化し続ける状況にあっても、クライアント側のフィッシング防護と新しい高度なフィッシング検知機能を組み合わせることで、フィッシングの成功をもっと的確に防げる適応手法について説明します。

コグニティブ手法を使ったフィッシングの検出と保護

この 10 年、フィッシングは急進的に変化して、詐欺の成功率を大きく上げ、オンライン・バンキング・アカウントの窃取と金融詐欺を可能にしました。

メール・コンテンツのこれまでにない巧妙化、高度な戦術、説得力のある甘言により、フィッシング・キャンペーンがうのみにされて、詐欺犯罪者は、専門知識に精通しているエンドユーザーでもだますことができます。

また、詐欺犯罪者は成功をさらに押し上げる多種多様な手法を開発してきました。たとえば、詐欺犯罪者がよく使う、ある総当たり攻撃では、数千ものシステムに侵入して 1 つのフィッシング・サイトをホストします。通常、一握りのシステムを随時起動して、定期的にサイトを切り替えることで、アンチフィッシング詐欺の調査員とバーチャルないたちごっこを繰り広げます。詐欺師はサイトを常に変更できるだけでなく、これらのサイトの DNS と IP アドレスをすぐに変えて相手をかく乱します。

APWG は 2016 年第 2 四半期の傾向レポートで、フィッシング・メールとフィッシング・サイトの継続的な増加を報告しています[6]。

この課題が大きくなるばかりなのは明らかです。では、詐欺にだまされないようにするにはどうすればいいのでしょうか？

IBM は特許取得済みの機械学習とフィッシング検知の高度な分析を使用することで、この課題に先見的に取り組んでいます。

これらの高度なフィッシング検知機能では機械学習を使って、リンク、画像、フォーム、テキスト、スクリプト、DOM (文書オブジェクト・モデル) データ、URL など、非構造化 Web サイト・データを分析します。これらの新機能と IBM® Trusteer® の強固な分析機能、他のグローバルなセキュリティー・インテリジェンス・データを組み合わせて、かつてない速さとスケールで金融機関の顧客を保護できます。

高度なアルゴリズムがインテリジェントに各種変数を評価して、正式なサイトとフィッシング・サイトを区別する高精度な脅威スコアを 生成します。

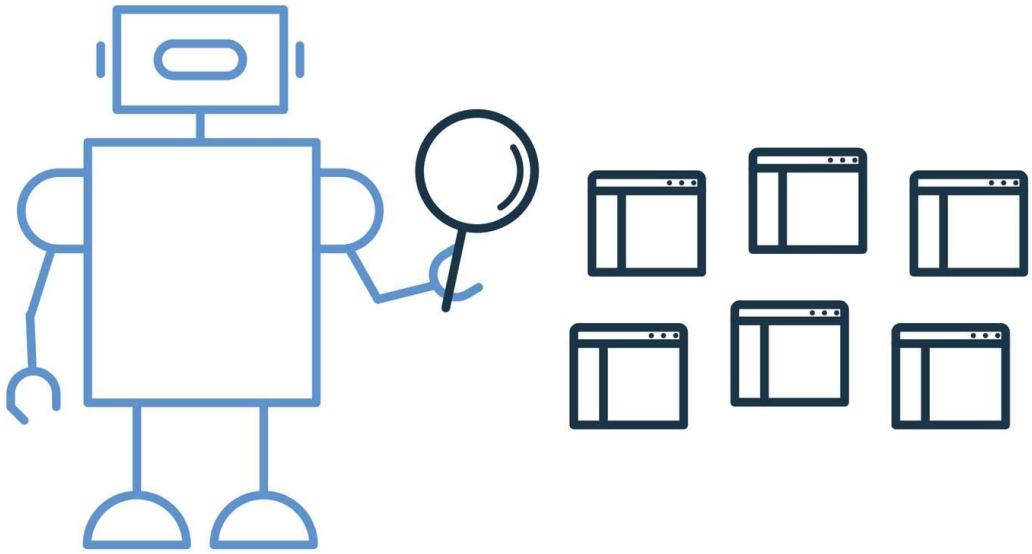
その結果、これらの先進的なフィッシング検知機能は、フィッシング検知のスピードを格段に速く上げ、新しいフィッシング戦術が始まった場合には組織が素早く適応できるように支援します。

たとえば、この手法では、″画像ベースのフィッシング″ など、従来のツールでは検知できない可能性がある新しいフィッシング傾向を素早く検知できます。画像ベースのフィッシングの場合、詐欺犯罪者は狙ったオンライン・バンキング・サイトのスクリーンショットを作成し、あとはエンドユーザーのログイン情報やクレジット・カード情報の入力に必要なテキストとフォームを追加するだけです。

新しいフィッシング攻撃の防止と適応

新しい不正オンライン・バンキング・サイトの検知しても、まだやることは残っています。特定した後、エンドユーザーがログイン情報をサイトに入力するのをストップするにはどうすればいいのでしょうか？エンドユーザーの知識がいかに豊富でも、人間である以上ミスを犯します。

検知



機械学習と高度な分析により、かつてないスピードとスケールでフィッシング・サイトを特定。

今日の多くの金融機関はフィッシング対策サービスを使って、フィッシング・サイトを検知しシャットダウンしています。ただし、これらの攻撃の性質上、サイトを立ち上げる詐欺犯罪者はすぐに検知されることを見越して攻撃方法を強化しています。

フィッシング対策サービスがフィッシング・サイトを検知してからブロックできるまでの時間差が、フィッシングがよく使用され攻撃方法として成功している理由の 1 つです。

IBM Trusteer Rapport® ソリューションは別の手法、つまり、銀行の顧客がフィッシング・サイトに移動するときにフィッシング攻撃から保護するように設計された手法を提供します。

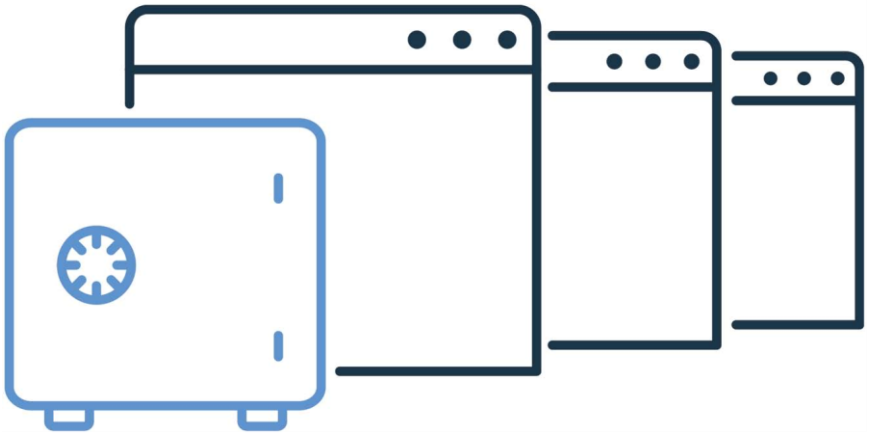
これは重要な特長であり、金融機関がフィッシング攻撃に費やすコストを削減できます。Ponemon Institute の評価によると、平均 1 万人の従業員がいる企業では 1 回の攻撃ごとにほぼ 370 万米ドルのコストがかかっています[7]。

エンドユーザーが Web サイトに移動すると、Trusteer Rapport ソリューションは疑わしいサイトを特定し、期間学習と高度な分析機能を使用して、サイトをリアルタイムで分析します。サイトがフィッシング・サイトであることが確定すると、エンドユーザーに通知するかブロックします。Trusteer Rapport ソリューションはフィッシングの罠をエンドユーザーに知らせることで、エンドユーザーの認証情報と決済カード・データの窃取を防ぎ、以降の詐欺行為の阻止を支援できます。

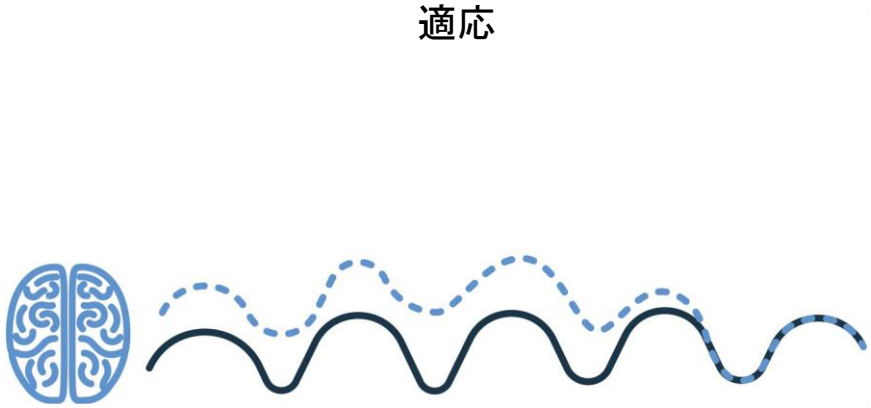
Trusteer Rapport ソリューションはエンドポイントに常駐しているので、エンドユーザーのプライベート・セキュリティー・ガードとして機能して、マルウェアの脅威をブロックし、特定されたフィッシング・サイトへのエンドユーザーのアクセスを防ぎます。

IBM の高度なフィッシング検知機能と IBM のセキュリティー・エキスパートによって生成された脅威情報を利用することで、このプラットフォームは、進化するフィッシング脅威に常に適応し続けます。

予防



Trusteer Rapport は、既知のフィッシング・サイトへのエンドユーザーのアクセスを防止。



新しいフィッシング戦術が登場すると、保護機能を素早くそれらの脅威に適応させる。

エンドユーザーからみると、このソリューションは簡単にダウンロードできてプライバシーを重視しているので、オンライン活動に安心して容易に取り掛かることができます。

結論

新しいフィッシング・サイトがオンライン・バンキングの顧客を狙ってまさに次から次へと現れます。フィッシング・サイトにアクセスしたエンドユーザーの多くは、ログイン情報や決済カード情報を詐欺犯罪者に開示する寸前だとは気付きもしません。

従来の手法だと、顧客の多くが認証情報を開示する前にサイトをシャットダウンすることはできないでしょう。

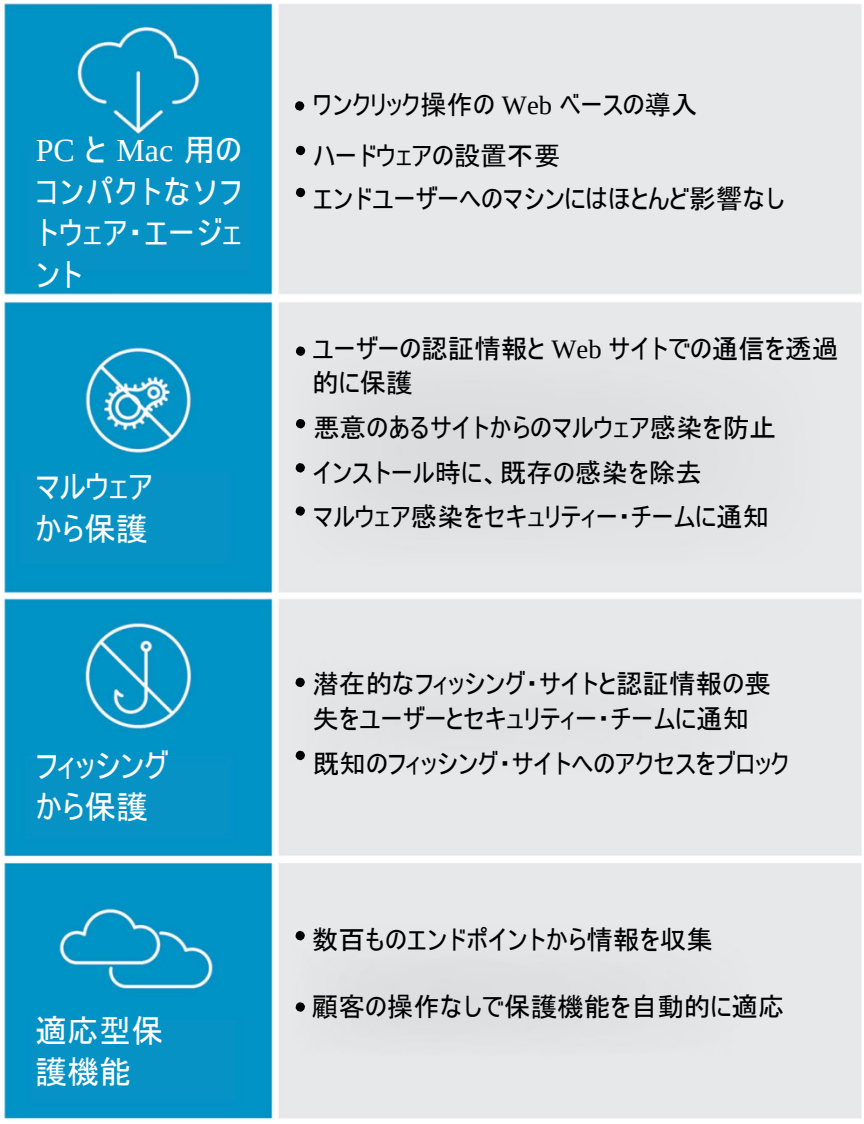
IBM は高度なフィッシング検知機能とクライアントベースの詐欺防護機能を組み合わせることで、フィッシング検知のスピードと精度を大きく前進させます。

IBM の手法では、Trusteer Rapport ソリューションをデバイスにインストールしてあるエンドユーザーを迅速に保護します。そのため、エンドユーザーは最も危険にさらされる情報開示時、フィッシング・サイトがシャットダウンする前に保護されます。

さらに、このソリューションは常に最新の状況に適応しているので、詐欺犯罪者が戦略と手法を変えるとそのことを検知して、保護機能をその変化に応じて調整します。

IBM を利用すれば、フィッシングによる金融詐欺にこれまでよりも簡単、迅速、効果的に立ち向かうことができます。

IBM Trusteer Rapport—特長



詳細情報

フィッシングの検知と保護に対する手法の改革については、IBM の担当者または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。**ibm.com**/security/trusteer

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
2017 年 3 月

[1] Marlo Aguilar「The Number of People Who Fall for Phishing Emails Is Staggering」Gizmodo、2015 年 4 月 14 日。Web サイトへのリンク: http://gizmodo.com/the-number-of-people-who-fall-for-phishing-emails-is-st-1697 725476

[2] Steve Zurier「91% of Cyberattacks Start With A Phishing Email」Dark Reading、2016 年 12 月 13 日。Web サイトへのリンク: http://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327 704?_mc=NL_DR_EDT_DR_daily_20161214&cid=NL_DR_EDT_DR_daily_20161214&elqTrackId=a66534266dff45aea858b9f0a66ad75b&elq=f95350c3de284618b8c9ab9f4f4257c8&elqaid=75468&elqat=1&elqCampaignId=24738

[3] Marika Samarati「4 eye-opening facts about phishing」IT Governance (ブログ)、2016 年 12 月 14 日。Web サイトへのリンク: http://www.itgovernance.co.uk/blog/4-eye-opening-facts-about-phishing/

[4] Tara Seals「84% of Phishing Sites Last for Less Than 24 Hours」Infosecurity Magazine、2016 年 12 月 12 日。Web サイトへのリンク: http://www.infosecurity-magazine.com/news/84-of-phishing-sites- last-for-less/

[5] Jonathan Crowe「Phishing by the Numbers: Must-Know Phishing Statistics 2016」(ブログ)。Web サイトへのリンク: https://blog.barkly.com/phishing-statistics-2016

[6] APWG. (2016 年 10 月 3 日)。APWG Phishing Trends Activity Report: 2nd Quarter 2016 [Trend Report].Web サイトへのリンク: https://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf

[7] Maria Korolov「Phishing is a $3.7-million annual cost for average large company」CSO Online、2015 年 8 月26 日。Web サイトへのリンク: http://www.csoonline.com/article/2975807/cyber-attacks-espionage/ phishing-is-a-37-million-annual-cost-for-average-large-company.html

WGW03271-JPJA-01