Case study

カーネギーメロン大学がフィッシングメール攻撃対策に多面的アプローチを採用

カーネギーメロン大学(CMU: Carnegie Mellon University)は、世界有数のComputer Scienceの研究・教育機関の1つです。この組織が証拠に基づく多層アプローチを用いてフィッシング攻撃からの防御を先導していることは驚くことではありません。

● 課題

現在、フィッシングと闘うため多面的アプローチを採用している組織が増え続けていますが、カーネギーメロン大学 もその1つです。
「他の多くの組織と同様に、私達はフィッシング攻撃による認証情報の喪失という継続的な脅威に直面しています」とCMUの情報セキュリティ担当ディレクター、メアリー・アン ・ブレア氏は述べています。

この職務に就いているブレア氏は、キャンパスコンピューティング及びネットワークインフラや機関情報のリアルタイム保護(トレーニング及びアウェアネスを含む)を担当しています。

「私達は、教職員だけでなく学生も含む当大学の全ての構成員について心配しています」とブレア氏 は述べています。

「こうした攻撃により、一人ひとりが個人的に個人情報の盗難に遭いやすくなります。コミュニティ全体を教育することは、CMUが良き市民であることの一環です」

カレッジ及び大学は、2つの理由で高リスクにさらされています。高等教育機関 は、詐欺メールを特定の組織内の従業員またはメンバーに送信する行為であるスピアフィッシングの一般的な標的になりつつあります。
「こうした詐欺行為は、(誘い込むための)罠、フィッシングメール、クリックスルーした時にランディングするサイトに関して、非常に巧妙になってきています」とブレア氏は述べています。

更に、特に被害に遭いやすいのが若年成人です。CMUで行われた研究では、18～25歳が特にフィッシング攻撃に引っ掛かりやすいことが明らかになりました。「したがって、ユーザコミュニティ全体の間でアウェアネスを高めることが重要です」とブレア氏は述べています。
「彼らは最後の砦です」

Carnegie Mellon

カーネギーメロン大学について

- ピッツバーグにメインキャンパスがあり、世界中に10箇所以上の学位授与キャンパスがある、国際的な私立研究大学
- 11,000名の学生、84,000名の卒業生、4,000名の教職員
- コンピュータ科学部(School of Computer Science)は、雑誌 (U.S. News & World Report)」の「America's Best Graduate Schools」で**全米1位にランク**されている
- 米国最大の大学を拠点とする**サイバーセキュリティ研究・教育センターの1つである**CyLab＊**を運営**している

＊CyLab: カーネギーメロン大学のコンピュータセキュリティ研究センター。2003年に設立され、大学内の異なる学部や学校の教員50人以上と大学院生100人以上が参加。CyLabは、サイバーセキュリティに関する事項について“CERT Coordination Center”及び“US-CERT”と協力している。(ウィキペディア)

● ソリューション

多面的アプローチの一環として、CMUはWombat Security Technologiesのアンチフィッシング製品のコンプリートスイートにライセンス供与しています。

Wombatの製品には、非常に効果的なアウェアネス・ツール及び教育ツールを組み合わせたもの — シミュレートされたフィッシング攻撃と、2つのインタラクティブ・トレーニング・モジュールである Anti-Phishing Phil® 及びAnti-Phishing Phyllis® — に加え、従来のアンチスパム/アンチウイルス・フィルタリング・ソリューションを補完する独自のアンチフィッシング・メールフィルタである PhishPatrol® が含まれています。

現在、Wombatにより世界中の数百万のユーザにライセンス供与されているこれらの製品は、金融、政府、電気通信、ヘルスケア、小売、教育、輸送、エネルギー、IT、及びサービス業界を含む幅広いバーティカル・マーケットにおける顧客組織によって導入されています。

ビジネスパートナー(一部)

IBM Security　KASPERSKY　RSA　CAMBRIDGE EDUCATION THE POWER OF KNOWLEDGE ISO 9001 : 2008 REGISTERED FIRM　TELSTRA

CDM INFOSEC AWARD WINNERS ★ 2017 ★

日本コーネット・テクノロジー株式会社
CORNET TECHNOLOGY (TEL) 03-5817-3655 (代)
www.nihon-cornet.co.jp

フィッシング判定: シミュレートされた攻撃が現実世界の脆弱性を明らかに

アウェアネスを高めることは、トレーニングプロセスにおける重要な第1段階です。ユーザが自分自身をより良く保護するのに必要なスキルを学習するためには、適切な時に適切な方法で教育が提供されなければなりません。この前提は、フィッシングについてのアウェアネスを高め、攻撃を回避するためのベストプラクティスを導入し、フォローアップ教育の基礎を築くWombatのシミュレートされた攻撃製品の成功の中心にあります。

SAAS(software-as-a-service): サービスとしてのソフトウェア製品であるWombatのシミュレートされたフィッシング攻撃により、IT管理者は、シミュレートされた攻撃をユーザに送信することによって、フィッシングに対するユーザの感受性を判定することができます。

ユーザが模擬フィッシングメールのうちの1つに引っ掛かると、システムはユーザの誤りを記録するだけでなく、今後はどうやって同様の攻撃に引っ掛かるのを回避するかをユーザに教えるリアルタイムの「ティーチャブル・モーメント(Teachable Moments)」をポップアップします。

＊ティーチャブル・モーメント: 受講者が模擬フィッシングリンクをクリックした際に瞬時に表示される教育ページ

「フィッシングについてユーザをトレーニングする従来の方法は、ユーザを怖がらせるためのものですが、これは、適切に行動するためのスキルセットをユーザに与えません」とブレア氏は述べています。

一例を挙げると、科学的研究では、**従業員は静的なサイバーセキュリティ・トレーニングメールに注意を払う気にならない**ことが示されています。組織が脅しの策略または座学に依拠する場合、ユーザはフィッシングメールに引っ掛かり続けるだけでなく、正当なメールを怖がるようになります。

これらのあまり魅力のないアプローチとは対照的に、Wombatのシミュレートされた攻撃は、気楽な ― ただし有益な ― ティーチャブル・モーメントを提供します。これらのジャストインタイムの教育実習は、今後の危険な行動を避けるための基本的なヒントを提供します。さらに、SaaSベースのプラットフォームには、組織が複数のフィッシングキャンペーンにわたってユーザの進捗を追跡するのを支援するレポート機能が含まれています。

結果を見れば、その効果が分かります― 500名の参加者がいた初期のシミュレートされたフィッシングキャンペーンでは、模擬攻撃に引っ掛かったユーザは、ティーチャブル・モーメントを読むのに平均で2分しかかかりませんでした。

しかし、これらの簡単なヒントでさえ、その後のフィッシングメールに引っ掛かった参加者の数を50%低減しました。

ユーザはメッセージを読み、そのメッセージを覚えていたのです。記憶をテストするために28日後に実施されたフォローアップキャンペーンでは、ブレア氏は、ユーザがティーチャブル・モーメントで見たヒントを覚えており、参加者がフォローアップのシミュレートされた攻撃に引っ掛かる確率が50%以下にとどまっていることに気付きました。

受け入れについてはどうでしょうか? ― ユーザは、「騙された気分になった」または「この方法に対して別の否定的な反応を抱いた」と報告しているでしょうか?答えは「ノー」です。「私達は、ユーザが抵抗を示すのではないかと心配していました」とブレア氏は述べています。「しかし、研究後の調査に回答した参加者の大半は、CMUがこの方法の使用を継続することを希望すると述べました。よって、私たちはこのツールのライセンスを購入しました」

シミュレートされたフィッシングキャンペーンを複数回繰り返すとより一層効果的であったため、その後の数ヵ月間で、大学は、学生集団を対象とした2つのカスタマイズされたキャンペーンを開始しました。「サイバー犯罪者はますますカスタマイズされるフィッシングメールを開発し続けているので、定期的なキャンペーンでユーザ集団を判定し続けることが非常に重要です」とブレア氏は付け加えています。

Anti-Phishing PhilとAnti-Phishing Phyllis: 1時間の講義よりも優れている10分のゲーム

毎週、大学がシミュレートされたフィッシング攻撃を開始することはできないので、ブレア氏は、Wombatのゲームベースのインタラクティブ・トレーニング・モジュールのうちの2つ、即ちAnti-Phishing Phil と Anti-Phishing Phyllis でキャンペーンを補っています。

特定のフィッシングメッセージに対するユーザの脆弱性を判定するシミュレートされた攻撃とは対照的に、これらのゲームは、キャンパス・コミュニティのメンバーがほんの数分で多数の例について学習することを可能にします。

詐欺URLを見分けることをユーザに教えるSCORM＊準拠ゲーム“Anti-Phishing Phil”

10～15分のプレイの間に、ユーザはこのゲームのデータベース内の豊富に揃ったURLから25個以上の異なるURLを判断するよう求められます。このモジュールのトレーニングコンポーネントは、ソーシャルネットワークを介して行われているかなりの数の攻撃など、現実世界のフィッシング傾向を反映しています。

＊SCORM(スコーム)とは、Sharable Content Object Reference Model(共有可能なコンテンツオブジェクト参照モデル)の略称で、eラーニングにおける共通化のための標準規格です。

Wombatのトレーニング方法は、サイバーセキュリティ教育の有効性を高めるのに役立つ、研究で実証された学習科学の原理に基づいています。特にユーザから賞賛を得ている対話型モジュールは、サイバーセキュリティに対する認識や行動を変え、組織のあらゆるレベルにおけるリスクを減らすのに役立ちます。

GARTNER'S MAGIC QUADRANT

日本コーネット・テクノロジー株式会社
CORNET TECHNOLOGY (TEL) 03-5817-3655 (代)
www.nihon-cornet.co.jp

査定と同様に、Wombatのトレーニング・モジュールには、セキュリティ専門家がユーザのパフォーマンスを追跡することを可能にする広範なレポート機能が含まれています。

- **“Anti-Phishing Phil” は、ユーザが将来のフィッシング攻撃に引っ掛かる可能性を著しく低減することが分かっています。**

（**Anti-Phishing Phil** を特集したサイエンティフィック・アメリカン(Scientific American)の記事「How to Foil ‘Phishing’ Scams」によれば、「このゲームをプレイした対象者が正当なURLを詐欺URLと区別する能力は、標準的な資料を用いてトレーニングした対象者の能力のおよそ2倍改善」しました。）

「私達は、CMUコミュニティ内の誰もがアクセスできるような方法でトレーニングを実施しています」とブレア氏は述べています。
このコンセプトをさらに強化するために、**Anti-Phishing Phil**は、**当大学の必修科目に組み込まれています**。1年生は全員、「Computing at Carnegie Mellon」と呼ばれる科目を修了する必要があります。そのオンライン学習環境の一環として、1年生はこのゲームをプレイし、資料の熟達度についてテストされます。「最も脆弱性がある集団は1年生です」とブレア氏は述べています。「時間とともに、1年生全員がこのプロセスを終えると、全学生がトレーニングされてこれらのスキルを身に付けることになります」

（**Anti-Phishing Phil** を補完するのは、CMUが追加トレーニング用に導入を計画しているもう1つのゲームベースのモジュールである Anti-Phishing Phyllisです。この10分のゲームは、詐欺メール内のフィッシングトラップを見つけることをユーザに教えます。）

トラップとしては、偽のリンク、悪意のある添付ファイル、賞金、機密情報を要求する「要返信」メールなどが挙げられます。Anti-Phishing Philの場合と同様に、このモジュールは、プレイヤーが自分自身をより良く保護することを学べるように、プレイヤーが見逃したトラップについてのフィードバックを即座にプレイヤーに提供します。

PhishPatrol: 従来のスパムフィルタ/ウイルスフィルタが見逃したものを捕らえる

CMUで最初にPhishPatrolを導入したのは”電気・コンピュータ工学部（Electrical and Computer Engineering Department）”でした。
この学部のメールフィルタリング・ソリューションは最新式であり、グレイリストを現在入手可能な最良のアンチスパムフィルタ及びアンチウイルスフィルタのうちのいくつかと組み合わせています。それでも、多くのフィッシングメールが通過し続けていました。

大半のメールフィルタは、フィッシングメールを捕らえるためにブラックリストに大きく依存しています。これらのリストは、体系的に数時間 — 場合によってはそれ以上 — 遅れています。大半のユーザはメールをその到着から数時間以内に読むので、標準的なフィルタは遅れずについていくことができません。

対照的に、WombatのPhishPatrolは、高度な機械学習技法及びメール機能の独特な組み合わせを使用してフィッシングを検出します。これにより、フィルタは、多くのゼロアワー（ゼロディ）攻撃を含め、他のフィルタによって検出されない多くのフィッシングメールを捕らえることができます。

「PhishPatrolは、誤判定なし・負荷の顕著な増加なしで、最小限の設定で
フィッシングメールのフィルタリングを改善することができました」
CMUネットワークマネージャ、Lou Anschuetz氏

PhishPatrolは、組織の既存のメールフィルタに取って代わるのではなく補完することを目的としています。
したがって、PhishPatrolは、アンチスパムフィルタ及びアンチウイルスフィルタと一緒に容易に導入できるように設計されています。

結果: ユーザに能力を与え、企業を保護する一連のツール

ブレア氏は、この多層の「カウンター攻撃」は同氏が保護する企業 — 及び人々 — に最も有用であると考えています。
「Wombatは我々のすぐ近くにあるので、当然のことながら、私の意見は少し偏っています」とブレア氏は述べています。

「しかし、CMUは別として、Wombatの背景を考えると、Wombatのアプローチは正真正銘のデータ主導型アプローチです。
Wombat製品はまさに人々がインターネットセキュリティにおいて見出している懸念に対処しようとしています」

「又、Wombat製品は科学の専門家による評価プロセスを経た研究の成果であり、その研究の成果は（専門家による）査読付き会議で発表されました。これは非常に珍しいことであり、Wombatのソリューションの有効性をよく物語っています」

実際、ブレア氏はWombatのツールに非常に感心したので、EDUCAUSE年次会議で自分の経験を仲間と共有することにしました。
この会議で、ブレア氏は、Wombat製品、特にシミュレートされたフィッシング攻撃を使用したCMUの成功について説明しました。

「話が終わる頃には、私達が何をどうやったかを知りたい人々の列がドアの外に続いていました」とブレア氏は述べています。
要するに、Wombatが行ったのは、最も賢いフィッシング詐欺師が行うこと、即ちユーザの行動に細心の注意を払い、その観察結果を利用して所望の行動に影響を及ぼすことです。

「最も重要なことは、正しい行動を実践するためのスキルセットを人々に与えることです。
人々にフィッシングメールを意識させるだけでは不十分で、正当なメールと詐欺メールを効果的に区別できることが必要です」
CMU、情報セキュリティ担当ディレクター、メアリー・アン・ブレア氏

日本コーネット・テクノロジー株式会社
CORNET TECHNOLOGY (TEL) 03-5817-3655 (代)
www.nihon-cornet.co.jp

Wombatの特長

無制限のプラットフォーム使用
追加料金なしで、ライセンス内の指定されたエンドユーザのメンバーがプラットフォーム・コンポーネントを無制限に使用することで、ROIを最大化します。

日本語を含む多言語サポート
約30種類の言語で判定やトレーニングが行えますので、多国籍企業や大学を含む国際教育機関等に於いては世界中で一貫したトレーニングが可能になります。

Wombat Wisdom
Wombat Wisdom Community、内部者グループ(Insiders group)、及び毎年開催されているWombat Wisdomユーザカンファレンスで直接/オンラインで、最も有能な人たちと繋がりを広めることができます。

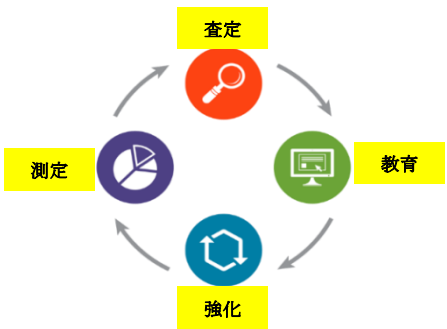
リアルタイムのレポート
広範囲にわたるエクスポート可能なユーザ分析、及びメトリックを用いて、判定やトレーニングの結果及び進捗の追跡が可能です。

受賞実績のあるサポート
・計画の作成時や、開始前後のサポートはライセンスに含まれているので組織に見合った効果的な計画の作成が可能です。
・使用中のサポートやサービスも全てライセンスに含まれているので追加料金は不要です。

Wombatの継続的トレーニング方法

GARTNER'S MAGIC QUADRANT

Wombat Security Technologies社のセキュリティ・アウェアネス(認識)及びトレーニングソリューションは、3年連続してGartner Magic Quadrant for Security Awareness Computer-Based Training Vendors のリーダーとなっています。



標準(Standard)の各教育モジュールは、平均約15分程度、Miniモジュールは5～7分程度で解けるようにデザインされています。Mobile対応モジュールは、時間や場所、デバイスに関わらず訓練が受けられます。

ミニモジュール

- ランサムウェアからの保護
- 移動時のセキュリティ
- USBデバイスの安全性

コンプライアンスに基づくトレーニング(標準モジュール)

- 個人を識別できる情報
- ペイメントカード業界データセキュリティ基準
- 保護医療情報

標準モジュール

- 電子メールのセキュリティまたはAnti-Phishing Phyllis ™
- URLトレーニングまたはAnti-Phishing Phil™
- ソーシャルエンジニアリング
- パスワードのセキュリティ
- 役員向けのセキュリティの要点
- データの保護と破壊
- セキュリティの要点
- モバイルデバイスのセキュリティ
- モバイルアプリのセキュリティ
- オフィス外でのセキュリティ
- 物理的なセキュリティ
- より安全なウェブブラウジング
- 安全なソーシャルネットワーキング

＊無料評価やデモのお問い合わせは下記まで

日本コーネット・テクノロジー株式会社
CORNET TECHNOLOGY (TEL) 03-5817-3655 (代)
www.nihon-cornet.co.jp