



proofpoint.

アダプティブ（適応型） WEB分離

URLベースのメール攻撃を阻止し、
ユーザーの生産性を維持するための、
人を中心としたアプローチ

人を中心とした脅威 ランドスケープ

データにとって最大の脅威は、サーバーのレガシーコードに隠れている欠陥でも、ダークWebで流通しているゼロデイエクスプロイトでも、未だにWindows 7が動いている古いPCでもありません。

最大の脅威はおそらく、あなたのデスクの近くに存在します。受付にきた訪問者であったり、倉庫にある段ボールであったり、またあなた自身であったりもします。

現在標的となっているのは、テクノロジーではなく人であり、組織にとって最大のリスクは人だからです。最新の攻撃は、ファイアウォールをすり抜けるのではなく、人の性質を利用します。攻撃者は従業員を騙して危険な添付ファイルを開かせたり、怪しいWebサイトへのリンクをクリックさせたりします。そして本物に見せかけたWebサイトを使って顧客を騙して、ログインクレデンシャルを盗むのです。

システムと違って、人にはパッチが当てられません。モノを守る技術を強化しても、人を標的にする攻撃を阻止することはできません。

テクノロジージャーナリストのRoss Kelly氏が言うように、セキュリティカメラを設置しても従業員による窃盗は解決しません。しかし問題の核心である「人」に取り組もうとすると、組織はインフラにフォーカスしたサイバーセキュリティ対策に注力してしまいがちです。¹

このガイドは今一度、人に注意を向けるお手伝いをするために、URL攻撃の仕組みとなぜその阻止が難しいのか、人を中心としたアプローチでそれをどう管理できるかを解説します。

コンテンツ

3 優位に立つ

5 カスタマイズ可能なコントロール



5 適応型の分離ソリューションの選択



サイドバー - ページ 5 ユーザーリスクの評価： VAPモデル

7 まとめ

1. Ross Kelly (Chief Executive Magazine). 「Almost 90% of Cyber Attacks are Caused by Human Error or Behavior. (サイバー攻撃の約90%は、人為的ミスや人の行動が原因となっています。)」 2017 年 3 月

メールは依然としてトップの攻撃経路

メールは、現在のビジネスコミュニケーションで中心的な役割を果たしているため、当然ながら他を大きく引き離してナンバーワンの脅威経路になっています。マルウェアの90%以上はメールで送付されており²、そしてその攻撃数は増え続けています。³

メールは最も多くの潜在的標的に、最も簡単に到達できる手段だからです。誰もがメールアドレスを持っており、ほとんどのビジネスはメールを使用していますが、メールはセキュリティを念頭に置いてデザインされていない、非常に古いアーキテクチャをベースにしています。

メール攻撃には様々な種類があります。多くの場合、攻撃者はメールに悪意のあるファイルを添付し、受信者を騙してそれを開けさせようとします。その他の場合では、危険なWebサイトへのURLリンクが埋め込まれていることもあります。このリンクは悪意のある添付ファイルをダウンロードさせようとしたり、またはログインクレデンシャルを入力させるフィッシングページにリダイレクトしたりします。

添付ファイルベース及びURLベースの攻撃数と割合は常に変化しています。しかし図1に示されるように、2019年に入ってからURL攻撃のほうが常に多い状態です。

攻撃タイプ別の1日当たりの悪意のあるメール数
(インデックス値：2018年第4四半期 - 2019年第1四半期)

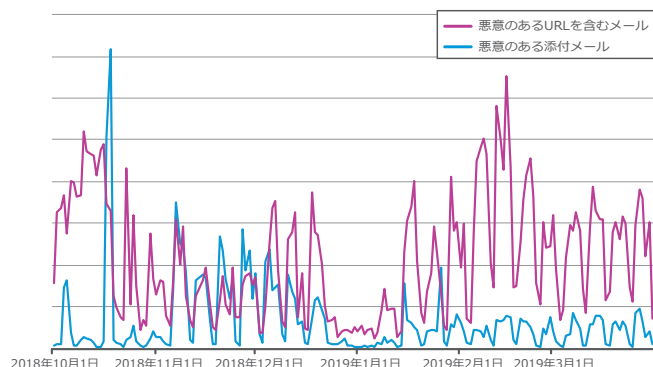


図1：攻撃タイプ別のトレンド（インデックス値）

URLベース攻撃の急増

従来型のセキュリティツールは、フィッシングを阻止するようにデザインされたものでさえ、現在のURLベース攻撃の急増には苦戦しています。最新の研究によると、フィッシングメールの4通に1通がOffice 365のフィッシング対策をすり抜けています。⁴

その理由は簡単です。悪意のある添付ファイルを用いる攻撃とは異なり、URLベースのメールキャンペーンには悪意のあるペイロードが付属していません。分析対象とすべきマルウェアが存在せず、既知のシグネチャとマッチさせることもできず、またサンドボックスで実行させることもできません。危険なプログラムの本体は、メール自身についているのではなく、URLの行き先であるWebサイトにあるからです。

脅威に対して優位に立つ

では、危険なURLを単純にブロックしてしまえばいいのでしょうか？しかし、言うは易く行うは難しなのです。新しいURLの作成は簡単のため、セキュリティツールによる分析やブロックリストの更新よりもはるかに早く作ることができます。そして危険なURLは、Bit.ly（安全とみなされている正規サービス）のようなリンク省略ツールを使えば簡単に見た目を偽装できてしまいます。そして悪意のあるコードは、DropboxやOneDriveのような、よく利用され信用されている有名なファイル共有サイトで簡単にホストすることができます。

また他の防御策が完璧だとしても、ユーザーの中にはメールに付いてきた危険なURLをクリックしてしまう人がいます。攻撃者は標的をリサーチする能力に長けており、ソーシャルエンジニアリングを用いて人の性質を利用します。ルアーの中には詳細な調査に基づいて巧妙に作成され、心理学的にも非常に効果が高いため、つい引っかかってしまうものもあります。

生産的でないアプローチ：ユーザーを取り締まる

安全が確認されている少数のURL以外をすべてブロックすることで、悪意のあるURLの問題を解決したいと思うセキュリティチームがあるかもしれません。またはユーザーのインターネット上での活動を監視して、危険なトラフィックを遮断することを検討しているチームもあるかもしれません。

しかしいずれのアプローチも、現在のビジネス環境には向いていません。

アクセスを確認済みのURLのみに制限すれば、ユーザーのストレスが高まり、反発を招きます。そして多くの場合、そのような対策はデータをより危険にさらすことになります。ユーザーは、セキュリティ保護対策（彼らにとっての障害物）を迂回するために、セキュリティの甘い個人デバイスや外部ネットワークを使って仕事をするようになるからです。

もしユーザーが我慢強くルールに従った場合でも、今度はIT部門にURL許可リストへの追加依頼が殺到します。リストを常に最新に保ち、かつユーザーからの大量の許可依頼に対応するのは、既に業務量過多状態のIT部門にとっては至難の業です。

また、ユーザーのインターネット上での活動を監視するのは、コストがかかるだけでなく、欧州の一般データ保護規則（GDPR）などのプライバシー規定違反になる可能性もあります。



アクセスを確認済みのURLのみに制限すれば、ユーザーのフラストレーションが高まり、反発を招きます。

2. Josh Fruhlinger (CSO). 「Top cybersecurity facts, figures and statistics for 2018（サイバーセキュリティの主要な事実と統計（2018年））」 2018年10月。

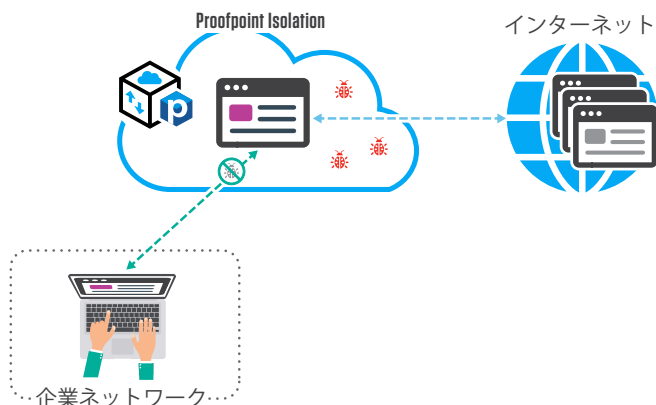
3. Proofpoint. 「Q1 Threat Report（第1四半期脅威レポート）」 2019年5月。

4. Warwick Ashford (ComputerWeekly.com). 「A quarter of phishing emails bypass Office 365 security.（フィッシングメールの4通に1通はOffice 365セキュリティをすり抜ける）」 2019年4月。

より良いアプローチ：Web分離

Web分離は、すべての人のニーズを満たせるアプローチです。この技術を用いると、ユーザーの個人的なインターネットの利用を企業ネットワークから切り離すことができます。

ユーザーは好きなブラウザを使って、好きなサイトを訪問できます。Web分離とは、HTMLコードをローカルPCで直接レンダリングするのではなく、リモートプロキシサーバを使ってユーザーのアクティビティを安全なコンテナ内で管理することです。高リスクなコンテンツ（実行コードを含む）は排除され、安全な状態のページがユーザーのブラウザに送られます。ユーザーが普段接している危険なコンテンツは、エンドポイントや企業全体まで到達しません。



Web分離により、ユーザーはプライバシーと自由を手に入れることができ、IT部門は不満や許可依頼から解放されます。またセキュリティチームは、個人のメールやインターネットブラウジングから発生する監視外のリスクに対応する必要がなくなります。

その他の利点には以下のようなものがあります。

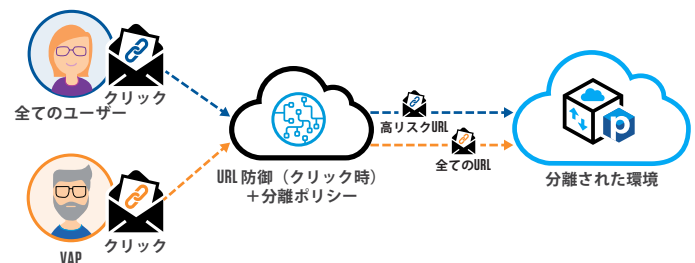
- ユーザーのプライバシーの確保（ユーザーの物理的位置が隠されるため）
- データ漏洩防止（分離された環境では、従業員は機密情報をアップロードできないため）
- 既存のセキュリティ対策への負荷が少ない（コードのスキャンやサンドボックス処理をする必要がないため）⁵

最良のアプローチ：アダプティブな分離

Web分離によって、個人メールの利用及びインターネット利用に関するセキュリティ問題を解決できますが、場合によっては制限が厳しすぎるということもあります。例えばマーケティング部門は広告エージェントから提供される写真をダウンロードするために、ファイル共有サイトを使う必要があるかもしれません。また購買部門は署名済みの請求書をベンダーのWebサイトにアップロードする必要があるかもしれません。

この場合、アダプティブな（適応型）Web分離が役立ちます。すべてのブラウジングセッションを分離して環境から隔離するのではなく、URLの安全性が確認された場合には分離セッションから戻って通常通りWebサイトを使用できるようにします。特定のURL、Webサイト分類またはユーザーに対して分離技術を用いることで、ユーザーの業務に支障を与えることなく脅威から環境を保護できるようになります。

アダプティブな分離は、既存のサイバー対策に追加できる柔軟な保護レイヤーです。選択的な適用が可能で、状況に応じて調整できます。例えば、最もリスクの高いユーザー（リスクは脆弱性、攻撃プロファイル、権限を基に決定）に対しては、メール内のすべてのURLを分離します。そうでないユーザーには、特定の分類のURLのみ分離します（分離セッションから戻れるオプション付き）。またユーザーのリスクプロファイルが変化した場合は、そのユーザーに対するコントロールを変更することもできます。



カスタマイズ可能なコントロール

人を中心とした最新の脅威ランドスケープ全体に対応できる汎用的なセキュリティなどというものは、存在しません。すべてのモノと人を、あらゆる状況下で同じように保護しようとすると、コストが高くなり、またリスクの低いユーザーに不必要な負担を強いることになります。

一方、人を中心としたアプローチは、ユーザー特有の脆弱性、攻撃プロフィール、そして権限に基づいて、そのユーザーに合ったセキュリティを適用します。全員を保護しながら、高リスクな人には特別な注意を向けるのです。高リスクな人とは、最も騙されやすい人、最も危険な攻撃の標的になる人、侵害された場合に最も被害の大きくなる役職の人です。

人を中心としたアダプティブなアプローチでは、ユーザーのリスクプロフィールが変わった場合はそれに合わせてセキュリティコントロールを柔軟に調整できます。日々変化する最新の脅威ランドスケープにおいては、このような柔軟性は非常に重要です。攻撃者は常に標的、手法、ツールを変化させています。そのため防御においても同じようなアプローチが取れなければいけません。

アダプティブな分離ソリューションの選択

アダプティブなセキュリティコントロールが必要なことは簡単にわかりますが、それに適した正しいソリューションを選択することは複雑です。

まずは人を中心とした防御にどのような知見が必要となるかを考えることから始めます。そしてその次に、適切な人に、適切なチャネルで、適切なタイミングで適切なコントロールを適用します。

人を中心とした知見と、正確な脅威検出

アダプティブな分離は、まずはどこに適用するべきかを明らかにすることから始めます。つまり、危険なURLの検出と、高リスクユーザーの識別から始めるということです。

最も効果的なソリューションは、URLベースの攻撃すべて（マルウェア脅威や非マルウェア型脅威を含む）を検出できます。

ユーザーリスクの評価：VAPモデル

人に個性があるのと同様、ユーザーがサイバー攻撃者にもたらす価値や雇用主に与えるリスクは人によって異なり、またデジタル上の習慣や弱点も人によって異なります。ユーザーは多様な手法を使った様々なレベルの攻撃の標的となっており、彼らの持つ仕事上のコンタクト先や、ネットワークやクラウド内のデータにアクセスできる特権が狙われています。

これらの要素を合わせると、そのユーザーのリスクを示すVAP（Vulnerability、Attack、Privilege：脆弱性、攻撃、特権）インデックスがわかります。

脆弱性

ユーザーの脆弱性評価は、その人のデジタル上の行動（どのように仕事をし、何をクリックするか）の評価から始めます。ユーザーはリモートで仕事をしたり、個人のデバイスから会社のメールにアクセスしたりします。またクラウドベースのファイルストレージを利用したり、クラウドアプリにサードパーティのアドオンをインストールしたりすることもあります。またはフィッシングメール攻撃に特に弱い人もいます。

攻撃

すべてのサイバー攻撃が同じというわけではありません。どの攻撃も被害を与える可能性があります。その危険度、洗練度、標的の絞り込み方は様々です。

無差別の「コモディティ化された」脅威は、他の種類の脅威よりも数は多いものの、よく知られていて阻止もしやすいため、危険度は低いと評価されます。他の脅威は、数は非常に少ないかもし

れませんが、洗練度が高く特定の人を標的としているため、より大きな危険を招く可能性があります。

特権

特権では、機密データ、財務上の権限、主要な人物との関係など、潜在的に価値のあるものへのアクセス権すべてを考慮します。これらのリスクは、攻撃者が得る利益や、侵害されたときに組織が被る被害を反映するものであるため、必ず計測しなければなりません。



マルウェア脅威には、ホストされたマクロ、感染させたコード、偽のアップデートインストーラなどが含まれます。非マルウェア型脅威には、フィッシングや詐欺Webサイトが含まれます。

どのような攻撃手法が用いられていても、ソリューションはその脅威を迅速かつ正確に検出できなければなりません。最も効果的なソリューションは、実践的な最新の脅威インテリジェンスを活用し、実際の脅威、進行中の攻撃キャンペーン、そして攻撃者のツール、手法、動機に対する詳細な知見に基づいて検出を行います。こういった知見は、どのURLを分離するか、ユーザーを分離セッションから戻しても良いか、制限対象外のWebページをロードしてよいか、ということ判断するために欠かせません。

ソリューションは危険なURLの検出に加え、どのユーザーがそういったURLのリスクにさらされているかも識別できなければなりません。つまり、誰が最も脆弱で、最も攻撃され、最も権限を持っているのかということの識別が必要なのです。

脆弱性の測定：人がどのように仕事をし、何をクリックするか

人の仕事の仕方から発生する脆弱性を評価します。これには、以下のような要素が考慮されます：

- どのクラウドアプリを使用しているか
- メールへのアクセスにはどのデバイスをいくつ使用しているか
- それらのデバイスは安全か
- ユーザーはデジタル上の予防策を実践しているか
- 多要素認証を常に使用しているか

脆弱性評価の次のステップは、ユーザーがフィッシングやその他のサイバー攻撃にどれほど騙されやすいかを判定することです。最良の方法は、フィッシングシミュレーションとセキュリティ意識アセスメントの成績を使うことです。

フィッシングシミュレーションメールを開いたり添付ファイルを開いたりするユーザーは、最も脆弱なユーザーです。これらを見放すユーザーは、上記のユーザーよりは危険度が低いとみなされます。そして不審なメールを発見した際にセキュリティチームやメール管理者に報告するユーザーは、最も脆弱性の低いユーザーです。

攻撃の評価：脅威の危険度は同じではない

リスクを数値化する際には、豊富な脅威インテリジェンスと最新の知見がカギになります。これを評価するにあたって重視すべき要素には以下が含まれます。

- サイバー犯罪者の高度さ
- 攻撃の拡散と集中の度合い
- 攻撃タイプ
- 全体の攻撃ボリューム

特権の測定：アクセス権がすべて

例えば、基幹システムや独占的な知的財産にアクセスできるユーザーは、特に攻撃に弱いわけでもなく、また攻撃者にまだ狙われていない場合でも、より厳しい分離コントロールが必要になることがあります。

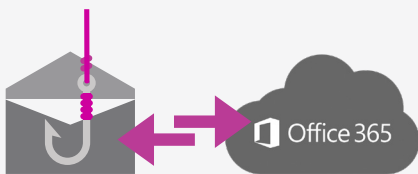
組織図の中でそのユーザーがどの位置にあるかということは当然、特権を評価する際の要素の一つです。しかし要素はそれだけではなく、またこれは一番重要な要素でもありません。攻撃者にとって、価値のある標的とは、攻撃者の求める役割を持つ人なのです。

プライバシーの保護

Web分離及び個人Webメールへの分離の主な利点には、ユーザーが自由にインターネットを利用でき、またユーザーのプライバシーを侵害することがないという点があります。

効果的な分離ソリューションは、GDPRの労働者のプライバシールールに準拠しなければなりません。また、ユーザーが分離されたブラウジングセッションを利用しているときは、そのアクティビティは完全に匿名化されていなければなりません。

当然、高リスクユーザーには、低リスクユーザーよりも厳しいセキュリティコントロールが必要です。しかし、どちらのユーザーも同等のプライバシー保護とブラウジングの権利を与えられるべきです。それを与えることによってリスクが高くなるわけではない場合は、特にそうです。



フィッシングメールのおよそ **4** 通に **1** 通が Office 365 のフィッシング対策をすり抜けています。

ビジネスを妨害するのではなく効率化する

効果的な分離ソリューションは、迅速な展開が可能で、そしてできる限りユーザーの作業の邪魔をしないようなものでなければなりません。

多くの場合、クラウドベースのサービスを用いると、展開が速く、かつ簡単に済みます。機敏なスケールアップが可能で、ユーザーが自分でプロビジョニングできるようなソリューションが最適です。

そして展開後は、実行されていることをユーザーに意識させないようなものでなければならず、また、ユーザーが自分の好みのブラウザ、設定、ブックマーク、カスタマイズを以前と同じように使えるようなものでなければなりません。言い換えると、ユーザーが技術に合わせるのではなく、技術がユーザーに合わせなければならない、ということです。

最後に、Web分離はWebコンテンツを安全、迅速、かつスムーズに提供できなければなりません。コンテンツとはビデオ、インタラクティブコンテンツ、Adobe Acrobat (PDF) ファイルなどを含みます。ユーザーの視点から見ると、リッチなWebサイトを表示できない分離技術は、単純にすべてブロックされているのと大して変わりません。

柔軟性

ほとんどの組織はWebを介して様々な外部組織とやり取りをしており、ユーザーがドキュメントのアップロードやダウンロードをするためにサイトへのフルアクセスを必要とする場合があります。

そのため、そのサイトのURLを分析して安全だとわかったら、ユーザーが分離環境から戻れるような分離ソリューションが必要です。こういった柔軟性があれば、ユーザーは環境に危険をもたらすことなく、業務に必要な作業を行うことができますようになります。

まとめ

現在の環境において、効果的なサイバーセキュリティを提供するにはテクノロジーではなく人にフォーカスしなければなりません。組織の保護は、人の保護から始まるのです。

Web分離（特にこのガイドで説明されているアダプティブな分離）は、急増するURLベースのメール攻撃に対抗するための効果的な手段になりえます。ユーザーの仕事の邪魔をせず、かつURLベースの脅威を効果的に阻止するソリューションを選択することが不可欠です。

Proofpointの人を中心としたピープル・セントリックなアダプティブアプローチの詳細はwww.proofpoint.com/jpでご確認ください。

Proofpointについて

Proofpoint, Inc. (NASDAQ:PFPT) はサイバーセキュリティのトップ企業であり、組織の最大資産と最大リスクである人を守ります。クラウドベースのソリューションの統合スイートによってProofpointは世界中の企業が標的型脅威を阻止し、データを守り、ユーザーがサイバー攻撃に対してより大きな耐性を持てるように支援します。また、Fortune 1000の過半数を超える企業を含む、あらゆる規模のトップ企業がメールやクラウド、ソーシャルメディア、Web関連の最重要なセキュリティとコンプライアンスのリスクを緩和するためにProofpointに頼っています。詳細はwww.proofpoint.com/jpをご覧ください。

©Proofpoint, Inc. Proofpointは、米国およびその他の国におけるProofpoint, Inc.の商標です。記載されているその他すべての商標は、それぞれの所有者に帰属します。