ソリューション概要

資格情報の盗難を防止

安全でないWebサイトから資格情報を盗み出す試みを阻止

侵害のおそれなくWebサイトを安全に閲覧

ユーザー アクセスを制限する、制約の多いITセキュリティ ポリシーを解消

資格情報の盗み出しは侵害を成功させる鍵

フィッシング攻撃は現代の企業に対するサイバーセキュリティ侵害の最も一般的な原因であり、従業員の資格情報は悪質な攻撃者にとって最大の標的です。資格情報は、企業を保護するために導入されている他の多数のセキュリティ プロトコルを突破する鍵となるからです。多くの場合、サイバー犯罪者と企業の貴重な知的財産の間に立ちはだかるのは、ユーザー名とパスワードの正しい組み合わせのみです。

スピア フィッシングが特に効果的なのは、自分の安全を守るはずの資格情報そのものを提供または更新してセキュリティ ポリシーを遵守しようとする、人間の能動的な行動を悪用する場合が多いからです。また、悪意のあるWebサイトは無数に存在し、存続期間も短いため、阻止するのも困難です。しかも、こうしたWebサイトのコンテンツは、正確な分類を回避するために頻繁に変更されます。

フィッシングは依然として組織に対して最も一般的で効果的なサイバー脅威

悪質なフィッシングの脅威は絶えず進化しており、さまざまな形を取っています。

- スピア フィッシング：個人の名前、役職、作業プロセスを記載して特定の個人を標的にする詐欺です。
- ホエーリング：企業の幹部を標的とし、法的通知、顧客からの苦情、経営上の問題を装っている場合が多くあります。
- ソーシャル エンジニアリング：人を信頼し、役に立とうとする人間の性質を悪用します。
- 不注意による感染：侵害されているニュースまたはソーシャル メディアのリンクを共有することで発生します。

フィッシング攻撃はさまざまな方法で行われます。

- 電子メール メッセージ内のフィッシング リンク
- ソーシャル メディア プラットフォーム上の標的型リンクまたはメッセージ
- チャット プログラムで共有されたリンク

HP SURE CLICK ENTERPRISE[1]は、悪意のあるサイトおよび評価の低いサイトでユーザーがログイン情報を共有しようとしたときに警告、阻止することで、資格情報の盗難を防止

Sure Click Enterpriseは、ユーザーが電子メール、チャット クライアント、PDF、またはその他のファイルに含まれるフィッシング リンクをクリックした後に、資格情報を搾取しようとするWebサイトでパスワードを入力できないようにすることで、資格情報の盗難を防ぎます。ユーザーがWebサイトにアクセスしてログイン資格情報の入力を求められたときに、Sure Click EnterpriseがHPのThreat Intelligence Serviceを利用してバックグラウンドでレピュテーション分析とドメイン分析を行い、サイトの安全性を判定します。安全性が確認されている正規のサイトであれば、ユーザーはソフトウェアによって妨げられることなく、通常どおりに資格情報を入力できます。

しかし、既知のフィッシング サイトの場合は、ユーザーがパスワードを入力しようとすると警告ウィンドウがページに重ねて表示され、サイトが資格情報を取得できないようになります。このソフトウェアを設定して、ユーザーがブラウザー ウィンドウを安全に閉じられるようにする、または、すべてのデータ取得フィールドを無効にした状態でサイトの閲覧を続行できるようにすることが可能です。

サイトの評価が低い場合、サイトを確認し、安全であるとわかっているサイトでない限り、資格情報を入力しないよう警告が表示されます。管理者は、このようなサイトに対して、資格情報の入力をブロックするか、ユーザーが自由に続行できるようにするかを選択できます。後者の場合は、ユーザーのPCで該当サイトがホワイトリストに登録され、今後同じサイトにアクセスした場合に警告が表示されなくなるため、不要な生産性の阻害を防ぐことができます。既知の不正なサイトまたは評価の低いサイトで行われた操作はすべて記録され、Sure Click Controllerに報告され、IT部門が脅威やユーザーの行動状況を確認します。

資格情報の保護：フィッシング詐欺による侵害を回避

フィッシング攻撃による資格情報の盗難を防止

従業員がフィッシング詐欺にだまされるリスクを軽減します。Sure Click Enterpriseは、既知の悪意のあるWebサイトでユーザーがログイン情報を入力することを阻止し、評価の低いすべてのサイトでリスクを伴う可能性がある行動についてユーザーに警告します。

ITセキュリティを合理化してコストを削減

HP Sure Click Enterpriseの高精度な警告によって、対応の選別時間を大幅に短縮し、偽陽性によるリソースの無駄使いを防止します。また、イメージの再作成、再構築、緊急パッチの適用を行う必要がなくなります。

リアルタイムの脅威インテリジェンスを共有

適応型のインテリジェンスを活用することで、防御をかいくぐろうとする攻撃も特定、阻止し、ネットワーク全体でリアルタイムの脅威データを共有して、SOCに完全なキルチェーン分析を提供します。

ハードウェアによって適用されるセキュリティで持続的な保護を実現

仮想化ベースのセキュリティを使用して、ハードウェアによるアプリケーション隔離を実現しているのはHP Sure Click Enterpriseだけです。最先端の検出ツールさえも簡単にすり抜けてしまう未知の脅威およびポリモーフィック型マルウェアに対しても有効です。

侵害の**67%**は資格情報の盗難が原因です。

– Verizon DBIR（2020年）[2]

資格情報の盗難に伴う侵害コストは、**平均386万ドル**、最大**836万ドル**に上ります。

– IBM『Cost of a Data Breach Report』（2020年）[3]

詳しくは、https://www.hp.com/enterprisesecurity/（英語サイト）を参照してください。

1. HP Sure Click Enterpriseには、Windows 10が必要であり、Microsoft Internet Explorer、Google Chrome、Chromium、Mozilla Firefox、および新しいEdgeに対応しています。Microsoft OfficeまたはAdobe Acrobatがインストールされている場合、サポートされる添付ファイルには、Microsoft Office（Word、Excel、PowerPoint）のファイルおよびPDFファイルが含まれます。
2. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2020/
3. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

4AA7-8573JPN、2020年10月、改訂1