Bromium

ソリューション概要

フィッシング攻撃を封じ込める

悪意のあるリンクであっても安全にアクセス

共有されたURLへのユーザー 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

ネイティブ ブラウザーのパフォーマンスと操作性で、フィッシング リンクから保護

多層防御をかいくぐり続けるフィッシング攻撃

フィッシング対策の技術や従業員のトレーニングが進歩しているにもかかわらず、フィッシング攻撃は広まる一方です。その理由は、非常に効果的な攻撃だからです。業務の遂行上、従業員はリンクをクリックせざるを得ず、ソーシャル エンジニアリングによってフィッシング リンクの識別が困難になっています。

フィッシング リンクが特に厄介なのは、悪意のあるWebサイトが無数に存在し、かつ存続期間が短いためです。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。これに加えて、従業員がよく考えずにリンクをすぐにクリックしたり、メール クライアントやチャット クライアントを開いたままにしたりすると、サイバー犯罪者が瞬時に入り込める経路が作り出されてしまいます。

悪意のあるペイロードを低コストかつ効果的に配信する方法

悪質なフィッシング リンクは絶えず進化しており、以下のようなさまざまな形態があります。

- 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
- 問題のない電子メール添付ファイルに含まれる悪意のあるリンク
- 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が、アプリケーション隔離によってフィッシングの脅威からホストを保護

HP Sure Click Enterpriseは、仮想化ベースのセキュリティを使用し、保護されたマイクロVM内のブラウザー タブですべての共有されたリンクを開くことで、組織をフィッシングの脅威から保護します。

ハードウェア強制の隔離によって、各ブラウザー タブは、ホストや他のすべてのブラウザー タブからも完全に隔離されるため、二次感染を防止できます。脅威が存在したとしても、ブラウザー タブを閉じると、マイクロVMとともに脅威も終了します。この完全なマルウェア キルチェーンはHP Sure Click Enterprise Controllerに送信され、ネットワーク上にある他のすべてのHP Sure Click Enterpriseデバイスと共有されるため、インフラストラクチャがさらに強化され、全体的な攻撃対象領域が減少します。

アプリケーション隔離：検出する前に防御

フィッシングの脅威を封じ込める

隔離されたマイクロVM内のブラウザー タブですべてのリンクを開きます。マルウェアが配布されたとしても封じ込められるため、ホストとネットワークが危険にさらされることはありません。従業員は安心してリンクをクリックできるようになりました。

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。

92%の組織が、フィッシング攻撃を特定して回避するトレーニングをエンドユーザーに対して実施しています。

—Wombat Security [1]

フィッシングは、ユーザーをだましてC2ソフトウェアやキーロギング ソフトウェアをインストールさせ、組織への認証や組織からのデータの抜き出しに必要な資格情報を搾取します。

—Verizon DBIR（2017年）[2]

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

1. https://www.wombatsecurity.com/press/press-releases/annual-state-phish-report-wombat-security-showssimulated-phishing-and-training
2. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

© Copyright 2020.HP Development Company, L.P.本書の内容は、将来予告なしに変更されることがあります。HP製品およびサービスに対する保証は、当該製品およびサービスに付属の保証規定に明示的に記載されているものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。ここに記載されている製品情報は、日本国内で販売されていないものも含まれている場合があります。本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対してHPは責任を負いかねますのでご了承ください。Microsoft、Windows、およびWindowsロゴは、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。Adobe®はAdobe Systems Incorporatedの商標です。Intel、Core、およびXeonは、米国およびその他の国/地域におけるIntel Corporationおよびその子会社の商標です。AMDおよびRyzenはAdvanced Micro Devices, Inc.の商標です。