ソリューション概要

悪意のあるドキュメントおよびファイルのダウンロードから保護

未知または未分類のWebサイトからドキュメントおよび実行可能ファイルを安全にダウンロードして開く

ネイティブ アプリケーションの実証済みのパフォーマンスと操作性で、悪意のあるダウンロードから保護

ダウンロードしたファイルへのユーザー アクセスを制限し、ワークフローを阻害するような制約の多いITセキュリティ ポリシーを解消

攻撃を受ける場合：悪意のあるダウンロードの発生源はさまざま

業務の遂行上、ユーザーは外部ソースからファイルをダウンロードしなければならない場合があります。また、ユーザーは共有ドキュメントをすぐにクリックする傾向があり、受信箱に届いてから平均4分以内にクリックしています。悪意のあるダウンロードは、以下のようにさまざまな手口で組織に侵入します。

- Web閲覧
- 共有リンクのクリック
- プログラムのインストール
- FTPファイル転送の開始

悪意のあるダウンロードが特に厄介なのは、不正なWebサイトが無数に存在し、かつ存続期間が短く、しかも正確な分類を回避するために、コンテンツの頻繁な変更を行っているからです。さらに従来のすべての検出方法をすり抜ける独自のポリモーフィック型マルウェアを配信しています。ファイルのダウンロードによるマルウェアの配布は効率的かつ低コストであり、常に進化しています。以下のようなさまざまな形態があります。

- **故意によるダウンロード：** ユーザーが通常のWeb閲覧中にドキュメントまたは実行可能ファイルのダウンロードを開始することがきっかけとなります。
- **実行可能ファイルの偽の更新プログラム：**ユーザーがWebサイトへのアクセス中に、だまされて悪意のあるファイルをダウンロードするように誘導されます。
- **ドキュメントへのリンク：**ユーザーは電子メールまたはチャット プログラムでドキュメントのリンクを受け取り、マルウェアが含まれるドキュメントのダウンロードに誘導されます。
- **URLのリダイレクト：**最初のリンクによってユーザーが別のURLにリダイレクトされ、ファイルのダウンロードに誘導されます。
- **不正なDNS：**DNSルックアップ レコードが侵害されると、ユーザーが問題のある行動を取らなくても、悪意のあるファイルをダウンロードしてしまう可能性があります。
- **偽のドライバーおよびユーティリティ：**ユーザーが「非公式の」ダウンロード サイトに誘導され、誤ってマルウェアをインストールしてしまいます。
- **水飲み場型攻撃：**標的がよく使用するWebサイトを攻撃者が感染させ、ファイル ダウンロードを置き換えたり、リダイレクトしたりします。

HP Sure Click Enterpriseが、アプリケーション隔離によって脅威のダウンロードから組織を保護

HP Sure Click Enterprise[3]は、仮想化ベースのセキュリティを使用して悪意のあるダウンロードから組織を保護します。HP Sure Click Enterpriseのアプリケーション隔離によって、すべてのダウンロード済みファイルが保護されたマイクロVM内で開かれます。

ハードウェア強制の隔離が使用されるため、ダウンロードされたドキュメントまたは実行可能ファイルがそれぞれ専用の安全なコンテナ内で実行されます。ファイルのダウンロードを介して配布された悪意のある脅威は、ホストや他のすべてのアプリケーションからも完全に隔離されるため、二次汚染を防止できます。アプリケーションまたはファイルを閉じると、脅威はマイクロVMとともに終了します。この完全なマルウェア キルチェーンが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

すべてのWebダウンロードを自動的に保護

ダウンロードされたすべてのドキュメントまたは実行可能ファイルを、ソース（HTTP/ HTTPS、FTPなど）にかかわらず安全に開きます。保護されたマイクロVM内にファイルが隔離されるため、使い慣れたユーザー エクスペリエンスを維持したまま安全にファイルをダウンロードしてアクセスできます。

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。

分析対象となったWebサイトの71%は存続期間が24時間以内にすぎず、その後恒久的に消滅します。これは悪意のあるコンテンツを配布し、検出を回避する場合に最適です。[1]

—Symantec

添付ファイルを最初にクリックするまでの中央値は3分45秒です。[2]

—Verizon DBIR（2017年）

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.symantec.com/connect/blogs/one-day-wonders-here-today-gone-tomorrow
2. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
3. 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。

© 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。