



ソリューション概要

悪意のある電子メール添付ファイルによる攻撃を阻止

OutlookまたはWebメールからの添付ファイルにマルウェアが含まれていても、ファイルを安全に開く

電子メールの添付ファイルへのアクセスを制限するような制約の多いITセキュリティポリシーを解消

従業員が電子メールの添付ファイルを開くことができるようにしてユーザーの生産性を向上

業務の遂行上、従業員は電子メールの添付ファイルを開く必要がある

従業員は、履歴書を読む、請求書进行处理する、配達通知を受け取る、財務諸表を共有する、法的な取り決めに関して外部の当事者とコラボレーションするなど、電子メール添付ファイルを日常的に使用します。また、安全らしいという判断で添付ファイルを開くことがよくあります。サイバー犯罪者はこの脆弱性を十分に認識していて、これを悪用します。

現在のランサムウェアは一般に、電子メールで送信される武器化されたMicrosoft OfficeドキュメントまたはPDFを介して配布されます。サイバー犯罪者がこれを行うのは、うまく行くからです。ランサムウェアに関連する2017年の推定損害額は50億ドル以上です。¹ 複数階層の防御を回避し、侵害した1台のホストから組織に侵入するための足掛かりを得るために、正当なアプリケーション（Microsoft Officeスイートなど、多くは明示的にホワイトリストに登録されています）を悪用することもできます。

マルウェア検出の進歩は有望であり、安全な電子メールゲートウェイが着実に改善され、ユーザーの意識向上トレーニングが増えているにもかかわらず、悪意のある電子メール添付ファイルは今なおあらゆる防御を突破していて、それがデータの侵害、消失、さらには破壊につながります。

電子メールで送信される現代の高度なマルウェアは、従来の検出から保護へという防御を完全に圧倒しています。

数値が示されています。

- 現在のマルウェアの99%はポリモーフィック機能を備えています。²
- 悪意のあるファイルの97%は、エンドポイントごとに完全に固有のものでした。³
- 2017年にはこれらの攻撃によるコストが23%増加しました。⁴

電子メールで配布されるマルウェアは低コストかつ効率的であり、絶えず進化している

現代のサイバー犯罪者は以下のものを使用しています。





- **ランサムウェア**：被害者のPC上のデータを対称鍵で暗号化し、被害者に身代金の支払いまたはマシンの再イメージ化を余儀なくさせます。ランサムウェアは蔓延していて、主に悪意のあるドキュメントを介して配布されます。
- **マクロを悪用したトロイの木馬**：悪意のあるバイナリをホストに投下します。その後、バイナリがリモートのコマンドアンドコントロールサーバーとの通信を確立してさらなる指示を受信し、追加の悪質なコードをダウンロードします。
- **ファイルレスマルウェア**：PowerShellなどのツールを悪用して、ホストにファイルを投下することなくコマンドを実行します。
- **悪意のあるリンク**：悪意のあるリンクは問題のない電子メール添付ファイルに隠され、複数階層の防御を簡単にすり抜けてドライブバイダウンロードまたはブラウザーエクスプロイトを引き起こします。

HP Sure Click Enterpriseが、電子メール添付ファイルに隠されたマルウェアをアプリケーション隔離により捕捉

HP Sure Click Enterpriseは、仮想化ベースのセキュリティを使用して、Microsoft OfficeドキュメントおよびPDFなどの電子メール添付ファイルを隔離されたマイクロVM内で開きます。マルウェアの起動と実行は可能ですが、マルウェアがエンドポイントまたはネットワークにアクセスできるようになることはありません。マルウェアは本質的にマイクロVMのコンテナに閉じ込められ、ユーザーが電子メール添付ファイルを閉じると廃棄されます。

マルウェアの実行を可能にすることで、デスク カルチャーが完全に変わります。エンド ユーザーは、ITセキュリティの制約について不満を述べるのではなく、誇りを持ってマルウェアの捕捉を報告するようになります。

アプリケーション隔離：検出される前に防御

	<p>電子メール添付ファイルを封じ込める</p> <p>すべての電子メール添付ファイルを隔離されたマイクロVM内で開きます。マルウェアが配布されたとしても封じ込められてアクセスできない状態になるため、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。</p>
	<p>ITセキュリティを合理化してコストを削減</p> <p>HP Sure Click Enterpriseの高精度な警告により、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。</p>
	<p>リアルタイムの脅威インテリジェンスを共有</p> <p>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。</p>
	<p>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</p> <p>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。</p>

成功したネットワーク侵入の**3分の2**は悪意のある電子メール添付ファイルに由来しています。

—Verizon DBIR（2017年）²

マルウェアの**47%**は、既存の複数階層の防御を回避できる新規のマルウェアまたはゼロデイ マルウェアです。

—WatchGuard⁵

「これは素晴らしい製品であり、自社のセキュリティを確保する上で非常に効果的です」

—ITシステムアナリスト
フォーチュングローバル
500の銀行⁶

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

1. <https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/>
2. <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>
3. <http://webroot-cms-cdn.s3.amazonaws.com/7814/5617/2382/Webroot-2016-Threat-Brief.pdf>
4. https://www.accenture.com/t20170926T072837Z_w/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
5. <https://www.helpnetsecurity.com/2017/09/29/credential-theft/>
6. TechValidate. <https://www.techvalidate.com/tvid/813-0A2-81D>
7. 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。

