HP WOLF SECURITY

脅威インサイトレポート

2022年第3四半期

脅威のランドスケープ

HP Wolf Security 脅威インサイトレポートの2022年第3四半期版へようこそ

四半期ごとに我々のセキュリティエキスパートが、HP Wolf Securityで特定された注目すべきマルウェアキャンペーン、トレンド、テクニックを紹介します。検知ツールを回避してエンドポイントに到達した脅威を隔離することで、HP Wolf Securityは、サイバー犯罪者が使用している最新のテクニックを把握し、セキュリティチームに新たな脅威と戦うための知識を与え、セキュリティ体制を向上させます。[1]

エグゼクティブサマリ

アーカイブとして配信されるマルウェア

44%

- マルウェアの配信に最もよく使われたファイル形式はアーカイブで、第2四半期と比較してサンプル数が11%増加し、初めてOfficeフォーマットを上回りました。
- 攻撃者は、悪意のあるペイロードをアーカイブやHTMLファイル内に暗号化することで、Eメールゲートウェイのスキャンなどのネットワーク境界のセキュリティ対策を回避しています。
- 脅威アクターは、PC上で悪意あるコードを実行するためにスクリプトベースのマルウェアを使用するようになっており、エンドポイントでの防御を回避するためにOS内蔵ユーティリティをますます利用するようになっています。
- 攻撃者は、HTMLスマグリングによってマルウェアを配信するために、有名ブランドやオンラインサービスを模倣し、効果的なソーシャル・エンジニアリングのテンプレートを作成することに、より多くの労力を費やしています。

特筆すべき脅威

マルウェア配信者は、システムへの感染にHTMLスマグリングの活用を進めている

2022年8月に停止した後、HP Wolf Securityは、9月上旬にQakBotマルウェアのキャンペーン活動の活発化を検知しました。QakBotは、脅威アクターがデータの窃取やランサムウェアの展開に使用してきた高機能のマルウェア・ファミリーです。[2] 注目すべきは、これらの新しいキャンペーンのほとんどが、システムへの侵入にHTMLスマグリングを利用しており、このマルウェア・ファミリーがよく利用する配信メカニズムが悪質なOfficeドキュメントから移行していることです。

これらのキャンペーンでは、PDFドキュメントを装った悪意のあるHTMLファイルがEメールで被害者に送信されました。HTMLファイルを開くと、ターゲットのWebブラウザに偽のオンラインドキュメントビューアが表示されます。WebページではZIPアーカイブがデコードされ、ユーザーにダウンロードを促します。

アーカイブは暗号化されており、ユーザーはWebページに表示されるパスワードを入力する必要があります。Eメールゲートウェイ・スキャナーなどのネットワーク境界のセキュリティ対策は、パスワードがなければ暗号化されたファイルを検査できないため、アーカイブ内のマルウェアが暗号化されることは攻撃者にメリットがあります。その結果、マルウェアを含む暗号化されたアーカイブは、ブロックされずにユーザーの受信トレイに到達する可能性がはるかに高くなり、感染が成功するリスクが高まります。

アーカイブの中には、悪意のあるショートカットファイル（LNK）が含まれています。このショートカットを開くと、悪意のあるコマンドが実行され、ダイナミックリンクライブラリ（DLL）の形でQakBotペイロードがダウンロードされ実行されます。マルウェアは、regsvr32.exe（T1218.010）を利用して動作します。regsvr32.exeはWindowsに組み込まれたDLLをOS内に登録するためのものですが、攻撃者が悪質なコードを実行するためによく悪用されます。[3]

今年初めに確認されたHTMLスマグリングと異なり、このキャンペーンのサンプルは、有名ブランドやサービスを悪用してユーザーを騙し、不正プログラムを実行させるテンプレートを使用しています。攻撃者は、最も効果的なルアーを見つけようと試行錯誤しており、HTMLスマグリングのデザインのバリエーションやブランドの悪用は、今後ますます加速していくと予想されます。

偽のオンラインドキュメントビューアは、脅威アクターの間で人気のあるルアー・テンプレートであることが判明しています。人手によるランサムウェア攻撃につながるマルウェアファミリであるIcedIDの配信者も、QakBotのテンプレートとほぼ同じものを採用してマルウェアを配信しています。

Documents

Image	Similarity Hash	Malware	Date	File Types
	003f3f3f3f3f0000	IcedID	2022-11-07	text/html
	003f3f3f3f3f0000	IcedID	2022-11-01	text/html
	3e3f3e3f3f3e0000	IcedID	2022-11-01	text/html

図1 - IcedIDのHTMLスマグリング・テンプレート

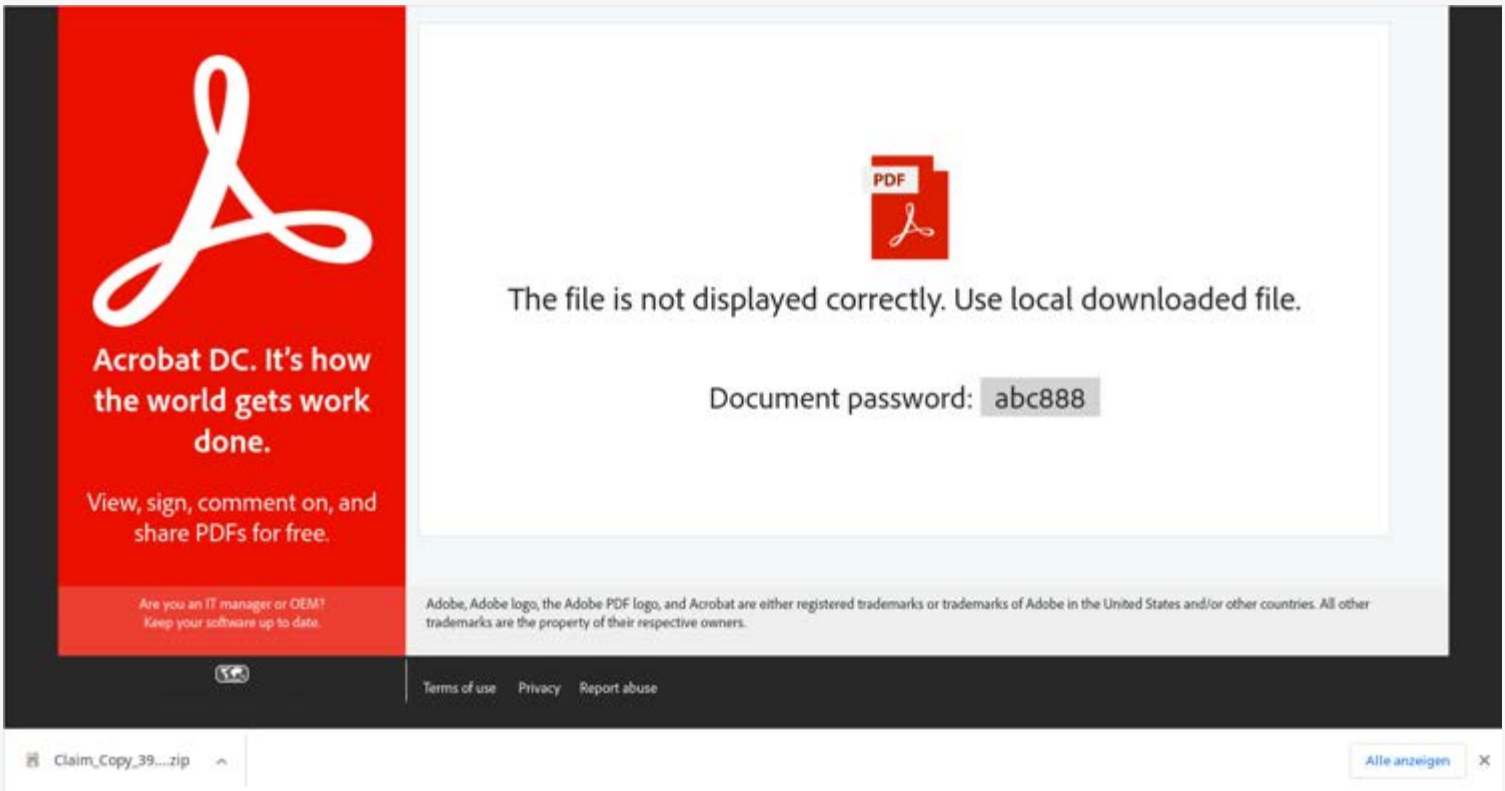


図2 - QakBotが侵入するために使用する偽のドキュメントビューア

ラテンアメリカのホテルにステルス型OpenDocumentマルウェアが展開

6月下旬、HP Wolf Securityは、OpenDocumentテキスト（.odt）ファイルを使用するC#で記述されたオープンソースのリモートアクセス型トロイの木馬（RAT）AsyncRATを拡散する異例のステルス型マルウェアキャンペーンを特定しました。[4] このキャンペーンは、予約申し込みを装ったEメールでラテンアメリカのホテル業界をターゲットとしたものでした。

OpenDocumentは、Microsoft Office、 LibreOffice、Apache OpenOfficeなどの一般的なオフィススイートと互換性のある、オープンなベンダーニュートラルなファイルフォーマットです。悪意のあるドキュメントは、Eメールの添付ファイルとして送信されます。ユーザーがこのドキュメントを開くと、他のファイルへの参照を持つフィールドを更新するかどうかを尋ねるプロンプトが表示されます。このプロンプトに対して"Yes"をクリックすると、Excelファイルが開かれます。

その後、マクロを有効にするか無効にするかを尋ねる別のプロンプトが表示されます。ユーザーがマクロを許可すると、これが感染チェーンの引き金となります。Exceldドキュメント内のVisual Basic for Applications (VBA) マクロはコンパクトで、Windowsに組み込まれたmshta.exe (T1218.005) ツールを使ったコマンドを実行し、Webからの追加コードをダウンロードし実行します。[5]

この時点で、PowerShell、VBScript、バッチスクリプトの複雑なチェーンが開始され、最終的にAsyncRATがデコードされ実行されます。[6] 感染したPC上でマルウェアを永続化するためにスケジュールタスクが作成されます。このタスクは、2時間ごとにマルウェアを再起動します。

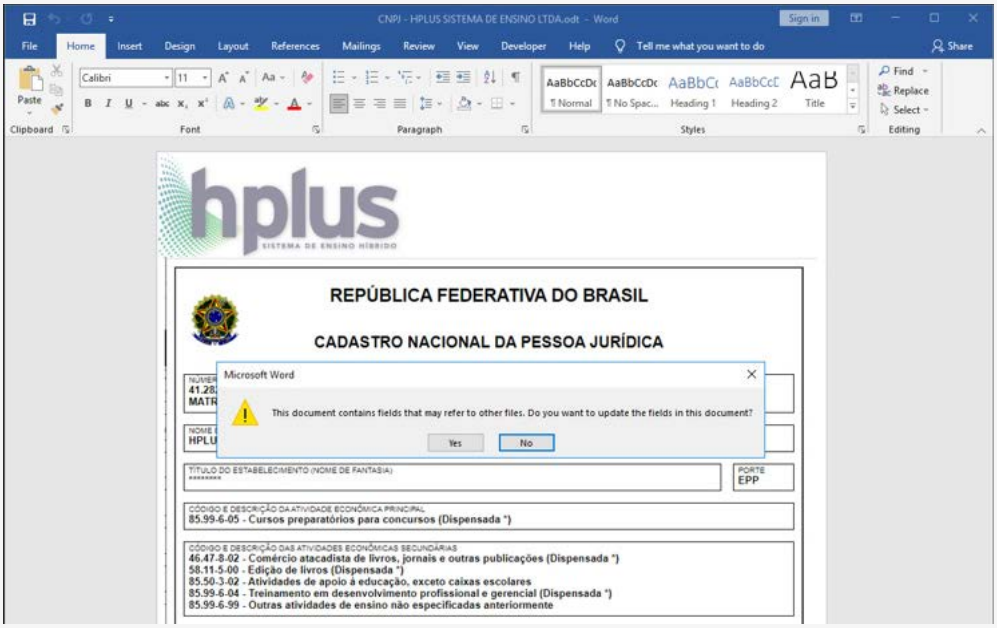


図3 - ドキュメント内のフィールドを更新するようユーザーに求めるルアードキュメント

多くの悪意のあるドキュメントとは異なり、OpenDocumentファイルを分析しても、隠されたマクロは見当たりません。しかし、このドキュメントは、リモートでホストされているOLEオブジェクトを参照しています。合計すると、webnar[...]infoというドメインでホストされている20のドキュメントが参照されています。

OpenDocumentファイルを使用してマルウェアを配布したことは、脅威アクターがキャンペーンでこのフォーマットを使用することがほとんどないため注目されました。また、VirusTotalにアップロードされた後、1週間以上にわたって検知率が0%であり、アンチウィルススキャナによる検知が上手くできなかったことも特徴的でした。

攻撃者は、エンドポイントセキュリティを回避してマルウェアを展開する目立たない方法を常に探し求めています。このキャンペーンは、OpenDocumentテキストファイルを悪用して、極めて低い検知率で外部OLE参照を通じてマルウェアを配信する方法を示しています。

Magniberと単一端末狙いのランサムウェアの脅威

近年、企業に対する「大物狩り(Big Game Hunting)」と呼ばれるランサムウェア攻撃は、その被害者の知名度や多額の身代金要求により、メディアの見出しを独占しています。しかし、単一端末狙いのランサムウェア（デバイス群ではなく、個々のコンピュータに感染するタイプのランサムウェア）は、依然として存在しています。

9月、HP Wolf Securityはホームユーザーを対象としたソフトウェアアップデートを装ったランサムウェアキャンペーンを隔離しました。このキャンペーンでは、被害者に2,500ドルを要求することで知られる単一端末狙いのランサムウェアファミリーであるMagniberが拡散されました。[7] 注目すべきは、攻撃者がランサムウェアをメモリ内で実行し、Windowsのユーザーアカウント制御（UAC）を回避し、Windowsの標準APIライブラリではなくsyscallを使用することで検知を回避するなど、巧妙なテクニックを使って検知を逃れていたことです。

感染チェーンは、攻撃者が管理するWebサイトからのWebダウンロードから始まります。ユーザーは、重要なアンチウイルスまたはWindows 10ソフトウェアのアップデートを装ったJavaScriptファイルを含むZIPアーカイブをダウンロードするよう要求されます。以前、MagniberはMSIファイルやEXEファイルを通じて拡散されていましたが、9月にランサムウェアの配信はJavaScriptに切り替わりました。

この攻撃者は、DotNetToJScriptのバリエーションを使用し、.NET実行ファイルをメモリ内にロードさせ、ランサムウェアがディスクに保存されないようにしています。[8] このテクニックは、ディスクに書き込まれたファイルを監視するセキュリティツールを回避し、感染システムに残るアーティファクトを減らします。

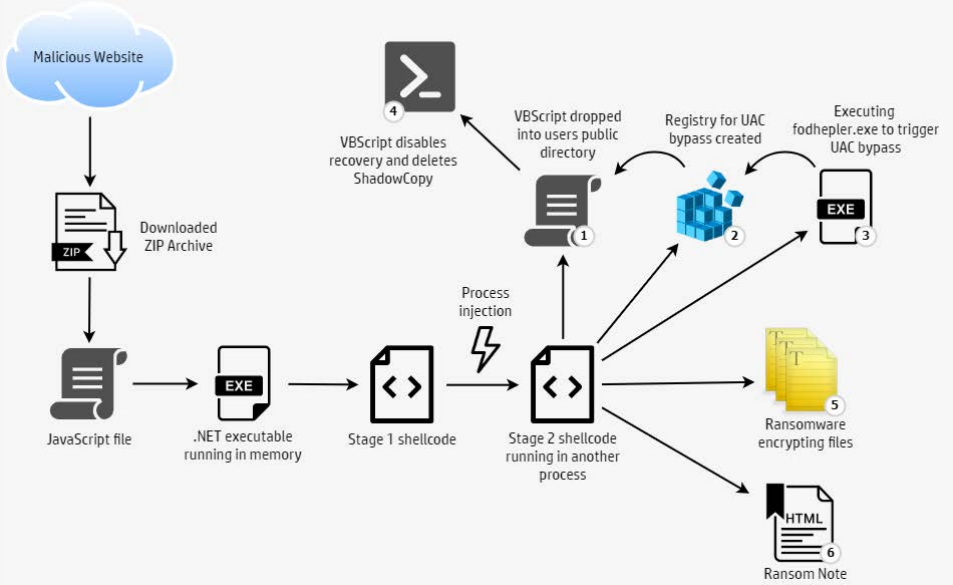


図4 - Magniberの感染チェーン

.NETコードはシェルコードをデコードし、別のプロセスにインジェクションします。ランサムウェアのコードはこのプロセスから実行され、まずシャドウコピーを削除し、Windowsのバックアップとリカバリー機能を無効にして、被害者のファイルを暗号化します。

Magniberは、被害者がデータを復旧できないようにするために管理者権限を必要とするため、マルウェアはfodhelper.exeを使用してユーザーアカウント制御（UAC）を回避し、ユーザーにアラートを発することなくコマンドを実行します。この機能を利用するためには、ログインしているユーザーがAdministratorsグループに属している必要があります。

興味深いことに、このキャンペーンにおけるMagniberのビルドは、Windows 11やプレリリース版を含む最近のバージョンのWindowsをサポートしています。これは、企業では古いOSを使用する傾向があるため、企業ではなくホームユーザーがこのキャンペーンの意図したターゲットであったことを示唆しています。

暗号化タスクのためにマルウェアはファイルを列挙し、そのファイル拡張子をリストと照らし合わせます。拡張子がリストにある場合ファイルは暗号化されます。最後に、マルウェアは暗号化されたファイルの各ディレクトリにランサムノート（身代金の要求）を置き、Webブラウザでノートを開き被害者にそれを示します。

モジュール型の感染チェーンがPCをRATや暗号通貨マイナーに感染させる

9月中旬、我々は、非常に複雑な感染チェーンをたどってシステムにマルウェアを感染させるキャンペーンを検知しました。このキャンペーンは、EメールとMicrosoft Wordの添付ファイルをターゲットに送信するという、ごく普通の方法で開始されました。送信者アドレスは信頼性を高めるために偽装され、添付ファイルはスパムフィルタをうまく回避してユーザの受信トレイに到達しました。

このドキュメントを開くと、埋め込まれたExcelスプレッドシートの読み込みを許可するかどうかをユーザーに尋ねます。許可された場合、スプレッドシートはmshta.exeを利用して、ファイル共有Webサイト上にホストされている悪意のあるエンコードされたファイルをダウンロードし実行します。これらのファイルは、シーケンス毎に違ったエンコードされたPowerShellやバッチスクリプト、または実行可能ファイルを含んでいます。

興味深いシーケンスの1つでは、PowerShellスクリプトが、セットアップ情報ファイル（INF）ファイルと別のPowerShellスクリプトを感染したシステムに保存します。その後、マルウェアは、内蔵のMicrosoft Connection Manager Profile Installer (cmstp.exe) ユーティリティを起動してINFファイルをインストールし、その中にリンクされているPowerShellスクリプトを実行します。

この結果、WindowsのAntimalware Scan Interface（AMSI）をバイパスして、バッチスクリプトを実行する別のPowerShellスクリプトが作成されます。このスクリプトは、Microsoft Defenderのファイルおよびプロセスの例外を定義し、ローカル管理ユーザーを作成し、侵入防止システムとローカルファイアウォールを無効にします。最後に、スクリプトは、Microsoft Defenderを停止しサービスを削除しようとします。

感染チェーンの他のシーケンスは、Agent Tesla、AsyncRAT、および暗号通貨マイナーの展開に使用されます。[9] 攻撃者は、このマルウェアキャンペーンのさまざまなコンポーネントをリモートのWebサーバ上でホストし、ペイロードのマルウェアを実行するためにさまざまなテクニックを使用しています。このようなモジュール型は、ペイロードを容易に交換でき、実行フローをキャンペーン中に変更できるため、攻撃者にとって有益です。

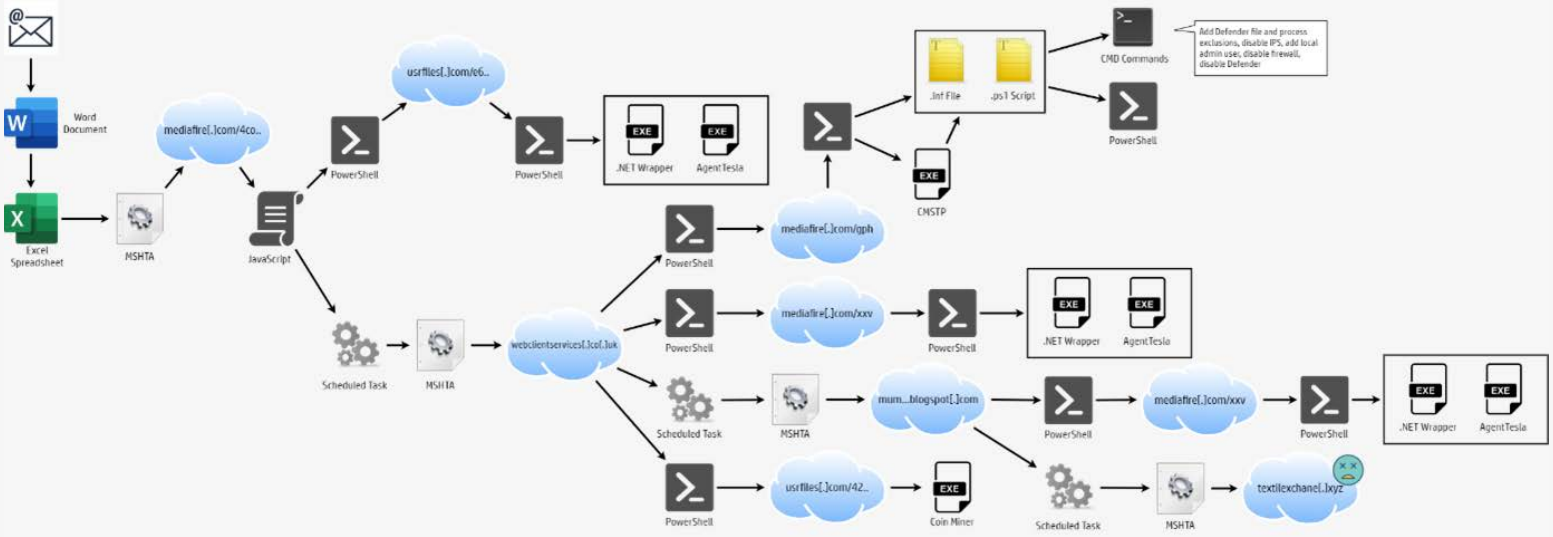


図5 - さまざまなペイロードにつながる感染チェーン

注目すべきテクニック

Magniberは署名検証をバイパスする

```
// SIG // Begin signature block
// SIG // MIIVnwYJKoZIhvcNAQcCoIIVkDCCFY
// SIG // DgMCGgUAMGcGCisGAQQBgjcCAQSgWT
// SIG // gjcCAR4wJAIBAQQQEODJBs441BGiow
// SIG // AAIBAAIBAAIBADAhMAkGBSsOAwIaBQ
// SIG // UmUvw3njbLzoyKW2oIISCjCCBW8wgg
// SIG // k7RgVZSNNqfJionWlBYwDQYJKoZIhv
// SIG // MAkGA1UEBhMCR0IxGzAZBgNVBAgMEk
// SIG // d3V4eSBTbTEQMA4GA1UEBwwHTXloam
// SIG // CgwRQ29tb2RvIENBIExpbWl0ZWQxIT
// SIG // ZyBRZXZ2b2tiYiBCZHVuamdxIE13dj
// SIG // MDAwMDBaFw0wNzQzMTIyMzU5NTlaMF
// SIG // AkdCMRgwFgYDVQQKEw9TZWN0aWdvIE
// SIG // BgNVBAMTJFNlY3RpZ28gUHVibGljIE
// SIG // ZyBSb290IFI0NjCCAiIwDQYJKoZIhv
// SIG // ADCCAgoCggIBAI3nlBIiBCR0Lv8WIw
// SIG // kSs+3H3iMaBRb6yEkeNSirXilt7Qh2
// SIG // toq9vQV/J5trZdOlDGmxvEk5mvFtbq
// SIG // S1uzuGQ2pH5KPalxq2Gzc7M8Cwzv2z
```

図 6 - 不正な Magniber の署名

Windowsのエコシステムでは、ダウンロードしたファイルは、Mark of the Web（MOTW）と呼ばれる指標を使用して、その起源に基づいてマークされます。[10] この機能により、Windowsは、ファイルがインターネットなどの危険な場所に由来するものかどうかを判断できます。ファイルの出所を追跡することは、ユーザーが信頼できない場所からのファイルを開いた場合にOSが警告を発することを可能にするために有用です。

警告が表示されない例外として、ダウンロードされたファイルがデジタル署名されている場合があります。2022年9月に見られたMagniberランサムウェアキャンペーンの分析中に、Webサイトからダウンロードされたにもかかわらず、JavaScriptファイルがそのような警告を表示しないことに気づきました。

このJavaScriptマルウェアを分析した結果、攻撃者はリスクのある出所の警告ダイアログを回避する目的で、不正なデジタル署名でファイルに署名していたことが判明しました。具体的には、署名には無効な証明書の日付や、セグメント長の定義と矛盾するオブジェクトの長さなど、複数の不正なフィールドが含まれていました。

不正な署名の結果、Magniberのサンプルはセキュリティ警告を引き起こさず、感染への障壁を取り除くことができました。

マルウェア配信に使われるファイルフォーマット

150

Officeフォーマットで配信されるマルウェア

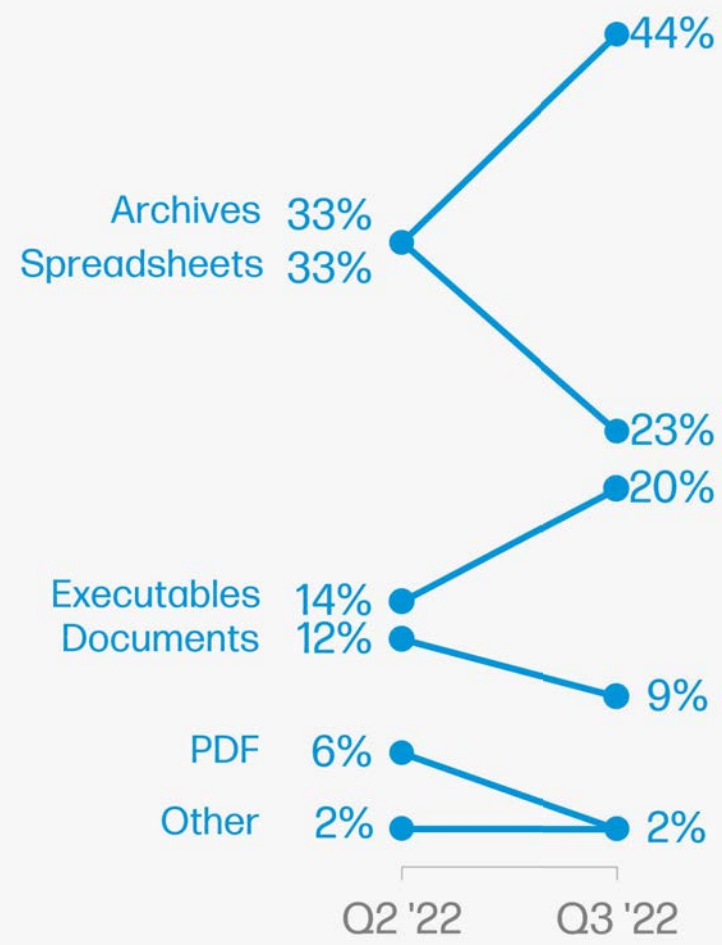
32%

注目すべきトレンド

アーカイブマルウェアが第2四半期に増加

11%

マルウェアのファイルタイプ



よく利用されるマルウェアのファイルタイプとしてアーカイブが悪意のあるドキュメントを抜く

第3四半期に、44%のマルウェアがZIPやRARなどのアーカイブファイルフォーマットで配信され、Officeフォーマット（第2四半期から13%減の32%）を抜いて、最も人気のあるマルウェアのファイルタイプとなりました。脅威アクターがスクリプトベースのマルウェアに移行する傾向が強まっているため、アーカイブフォーマットの人気は2022年に急増し、第1四半期から25%上昇しました。アーカイブは簡単に暗号化できるため、Webプロキシ、サンドボックス、メールスキャナによるマルウェアの検知が難しく、脅威アクターにとって魅力的な存在です。さらに、多くの組織が正規の理由で暗号化アーカイブを使用しているため、ポリシーによって暗号化アーカイブのメール添付を拒否することが困難になっています。その結果、アーカイブは攻撃者がユーザーの受信トレイに到達する能力を高め、悪意のあるコンテンツの検知をスキャンに依存するセキュリティ管理策を回避します。

Eメールは依然として最も危険な配信ベクター

HP Wolf Securityが検知した脅威の69%はEメール経由で、第3四半期も引き続きマルウェアの配信ベクターとして上位を占めています。実際、潜在的に迷惑なアプリケーション（PUA）を除くと、脅威の88%はEメールで送信されており、この経路がほとんどのユーザーにとっていかに危険であるかを如実に示しています。第3四半期は、第2四半期と比較して、Webブラウザのダウンロードによって配信された脅威が1%増加し、その他の経路が1%減少しました。

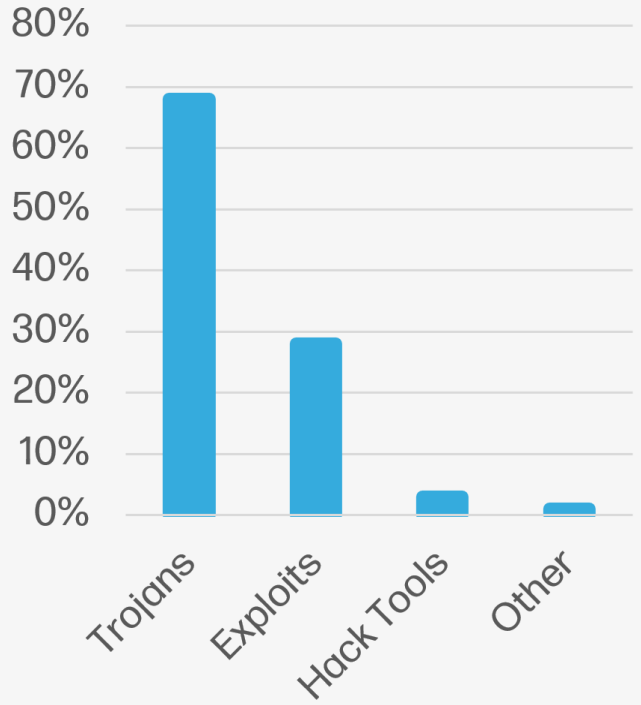
脅威の侵入経路

69%
Eメール

18%
Webブラウザーダウンロード

13%
その他

マルウェアのタイプ



最新の状態を維持する

HP Wolf Security 脅威インサイトレポートは、ほとんどのお客様が脅威のテレメトリをHPと共有することを選択することによって実現されています。当社のセキュリティ専門家は、脅威の傾向や重要なマルウェアキャンペーンを分析し、洞察を注釈したアラートを顧客にフィードバックしています。

HP Wolf Security の導入を最大限に活用するために、お客様には以下のステップを踏むことをお勧めします。[a]

- HP Wolf Security ControllerでThreat Intelligence ServicesとThreat Forwardingを有効にし、MITRE ATT&CKのアノテーション、トリアージ、専門家による分析を受けることができるようにしてください。[b] 詳細については、ナレッジベースの記事をご覧ください。[11 12]
- HP Wolf Security Controllerを最新の状態に保ち、新しいダッシュボードとレポートテンプレートを受け取ることができるようにしてください。最新のリリースノートとソフトウェアのダウンロードは、カスタマーポータルでご覧ください。[13]
- HP Wolf Securityのエンドポイントソフトウェアをアップデートし、当社の研究チームが追加した脅威アノテーションルールを常に最新に保ってください。

HP Threat Research チームは、セキュリティチームが脅威から身を守るために役立つ 侵害の痕跡 (IOC) やツールを定期的に公開しています。これらのリソースは、HP Threat Research GitHub リポジトリからアクセスできます。[14] 最新の脅威に関する調査については、HP WOLF SECURITY ブログ [15] にアクセスしてください。

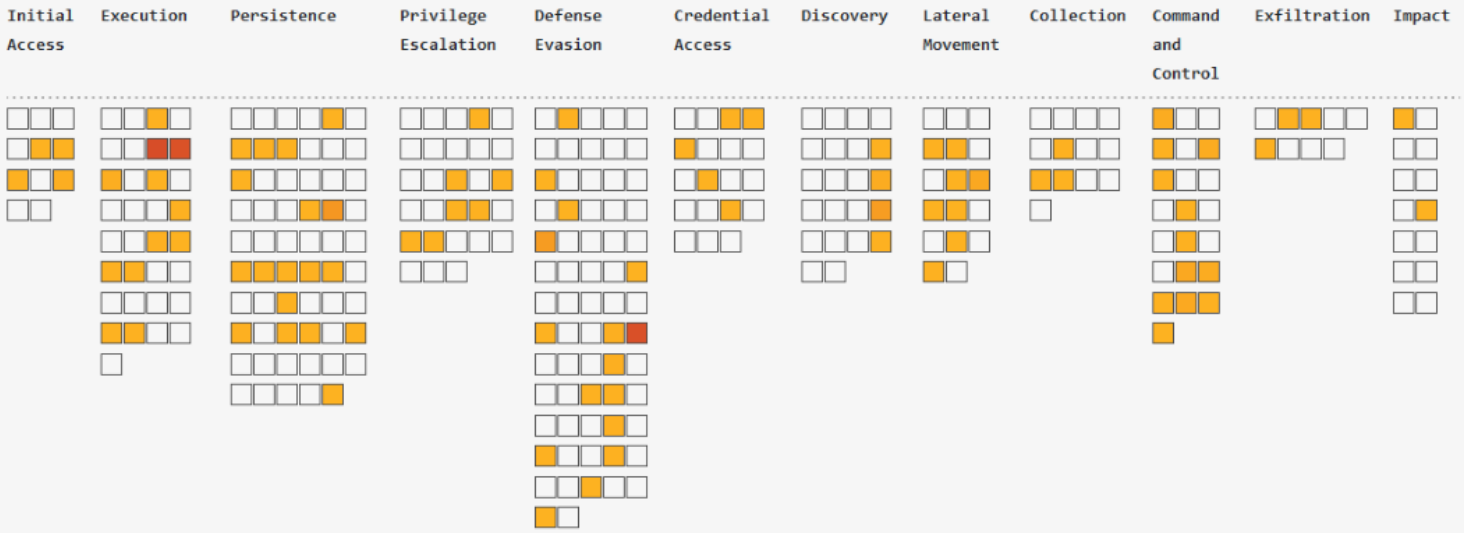


図7 - 2022年第3四半期に使用された攻撃テクニックの分布を示すMITRE ATT&CKのヒートマップ [16]

HP Wolf Security 脅威インサイトレポートについて

企業は、ユーザーがEメールの添付ファイルを開いたり、Eメール内のハイパーリンクをクリックしたり、Webからファイルをダウンロードすることに対して最も脆弱です。HP Wolf Securityは、リスクの高いアクティビティをマイクロVMに隔離し、ホストコンピュータがマルウェアに感染したり、企業ネットワークに広がったりしないようにすることで企業を保護します。HP Wolf Securityは、イントロスペクションを使用して豊富なフォレンジックデータを収集し、お客様のネットワークが直面する脅威を理解し、インフラストラクチャを強化できるよう支援します。HP Wolf Security 脅威インサイトレポートは、当社の脅威研究チームが分析した注目すべきマルウェアキャンペーンを紹介し、お客様が新たな脅威を認識し、環境を保護するために行動を起こすことができるようにします。

HP Wolf Securityについて

HP Wolf Securityは、新しいタイプ[c]のエンドポイントセキュリティです。HPのハードウェアで強化されたセキュリティとエンドポイントに特化したセキュリティサービスのポートフォリオは、組織がPC、プリンター、そして人々をサイバー犯罪者から守るために設計されています。HP Wolf Security は、ハードウェアレベルからソフトウェアやサービスに至るまで、包括的なエンドポイントの保護とレジリエンスを提供します。

リファレンス

[1] https://hp.com/wolf

[2] https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot

[3] https://attack.mitre.org/techniques/T1218/010/

[4] https://threatresearch.ext.hp.com/stealthy-opendocument-malware-targets-latin-american-hotels/

[5] https://attack.mitre.org/techniques/T1218/005/

[6] https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat

[7] https://malpedia.caad.fkie.fraunhofer.de/details/win.magniber

[8] https://github.com/tyranid/DotNetToJScript

[9] https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

[10] https://attack.mitre.org/techniques/T1553/005/

[11] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding

[12] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence

[13] https://enterprisesecurity.hp.com/s/

[14] https://github.com/hpthreatresearch/

[15] https://threatresearch.ext.hp.com/blog

[16] https://attack.mitre.org/

LEARN MORE AT HP.COM

HP WOLF SECURITY

a. HP Wolf Enterprise Securityはオプションサービスで、HP Sure Click EnterpriseやHP Sure Access Enterpriseなどが該当します。HP Sure Click Enterpriseは、Windows 10が必要で、Microsoft Internet Explorer、Google Chrome、ChromiumまたはFirefox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、サポートされている文書には、Microsoft Office（Word、Excel、PowerPoint）およびPDFファイルが含まれます。HPSure Access Enterpriseには、Windows 10 ProまたはEnterpriseが必要です。HPのサービスは、ご購入時にお客様に提供または提示される、当該HPのサービスに適用される使用条件に準拠します。お客様によっては該当地域の法令に従ってその他の法的権利を有することもあり、その場合には当該権利はHPサービスお取引条件またはお使いのHP製品とともに提供されるHP限定保証条件による影響を一切受けません。完全なシステム要件については、以下を参照ください。www.hpdaas.com/requirements

b. HP Wolf Security Controllerは、HP Sure Click EnterpriseまたはHP Sure Access Enterpriseが必要です。HP Wolf Security Controllerは、デバイスやアプリケーションに関する重要なデータを提供する管理・分析プラットフォームで、スタンドアロンサービスとしては販売していません。HP Wolf Security Controllerは、厳格なGDPRプライバシー規制に従っており、情報セキュリティに関してISO27001、ISO27017、SOC2 Type2の認証を受けています。HPクラウドへの接続が可能なインターネットアクセスが必要です。完全なシステム要件については、以下を参照ください。www.hpdaas.com/requirements

c. HP SecurityはHP Wolf Securityになりました。セキュリティ機能はプラットフォームによって異なりますので、詳細は製品データシートをご覧ください。

HPのサービスは、ご購入時にお客様に提供または提示される、当該HPのサービスに適用される使用条件に準拠します。お客様によっては該当地域の法令に従ってその他の法的権利を有することもあり、その場合には当該権利はHPサービスお取引条件またはお使いのHP製品とともに提供されるHP限定保証条件にによる影響を一切受けません。