HP WOLF SECURITY

脅威インサイトレポート

2022年第4四半期

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4四半期版へようこそ

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ー

メールゲートウェイのセキュリティを回避したEメール脅威

13%

特筆すべき脅威

攻撃者はPDFルアーでマルウェアを配信し、Eメールのセキュリティを回避

- 連続3四半期間アーカイブはマルウェア配信の最も人気のあるファイルタイプでした (42%)。攻撃者がOfficeファイル形式からディスクイメージファイル(IMG、ISO)等のマクロ非依存の選択肢にシフトしているため、アーカイブマルウェアは第1四半期から20%増えています。
- 第4四半期は、人気のあるソフトウェアプロジェクトを模倣し、ユーザーを騙してPCをマルウェアに感染させる攻撃者が急増しています。この攻撃は、ユーザーが検索エンジンの広告をクリックすると、正規のWeb サイトとほとんど同じように見える悪意のあるWebサイトへ誘導されることを利用しています。
- 攻撃者は、PDFファイルに悪意のあるリンクを埋め込むことで、Eメールゲートウェイスキャナー等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。HP Wolf Securityが特定したEメールの脅威の13%は1つ以上のEメールゲートウェイスキャナを回避しており、検知ベースのセキュリティ対策に頼ることの限界を浮き彫りにしています。
- 脅威アクターは、被害者からクレジットカードやデビットカードの情報を盗むために、QRコードを使ったルアーを試しています。この種の攻撃では、対象者がフィッシングに対する保護が不十分な携帯電話から悪意あるWebサイトにアクセスする可能性が高くなります。

PCへのマルウェア配信手法としてOfficeドキュメントやスプレッドシートが使われなくなったことで、攻撃者はHTMLスマグリングや悪意あるショートカット (LNK)ファイルなどの代替手法を試すようになりました。 HTMLスマグリングは、メールゲートウェイのセキュリティ回避に有効です。これは攻撃者がマルウェアをHTML添付ファイル内に暗号化することで、スキャナによる悪意あるコンテンツの検査を防止できるからです。この手法は依然として用いれれていますが、攻撃者は常に新たなテクニックを駆使して検知を回避しようとしています。12月に勢いを増したテクニックの1つが、PDFドキュメントです。HP Wolf Securityでは、第4四半期にPDFマルウェアが前四半期比で38%増加したことを確認しています。

感染チェーンは、攻撃者がPDFドキュメントを被害者にEメールで送信することから始まります。HTMLスマグリングと同様に、攻撃者は受信者の注意を引くために有名ブランドを模倣します。図1は、第4四半期に見られた偽のオンラインドキュメントビューアの例(人気のあるルアーテンプレート)です。このPDFドキュメントには、Webサーバ上でホストされているZIPアーカイブファイルへ導くリンクが含まれています。このPDF添付ファイルには実行可能なコードが含まれていないため、メールゲートウェイで検知される可能性は低くなっています。また、検知を回避する可能性を高めるため、攻撃者はアーカイブを暗号化し、受信者に送信されるPDF文書でパスワードと手順を提供します。

多くのダウンロードされたZIPアーカイブには、ショートカットファイルを含むディスクイメージファイル(.ISOまたは.IMG) が含まれています。感染を引き起こすためには、受信者がショートカットファイルを開く必要があります。このテクニックは、人手によるランサムウェア攻撃の先駆けとして知られるQakBotやIcedIDなどのマルウェアファミリーの配信に用いられていることが確認されています。[2 3]

悪意のあるPDFやHTMLの添付ファイルを介して感染させるための手順は、マクロが有効なOffice文書よりも多くなっています。しかし、マルウェアの実行に多くのユーザー操作が必要であるにもかかわらず、攻撃者がネットワークの侵害に成功しているのは、ユーザーがこうした罠に引っかかってしまうからです。

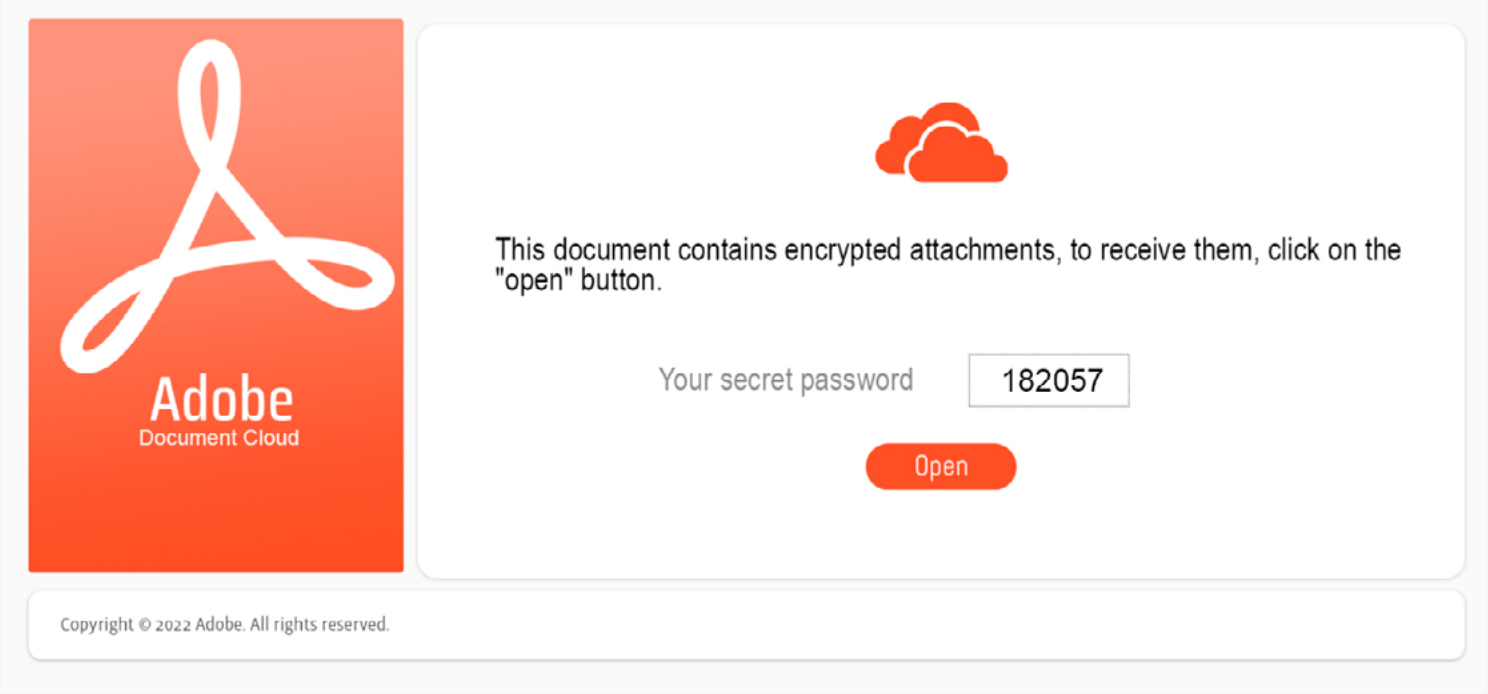


図1- 被害者を騙してシステムをQakBotに感染させるために使用される偽のドキュメントビューア

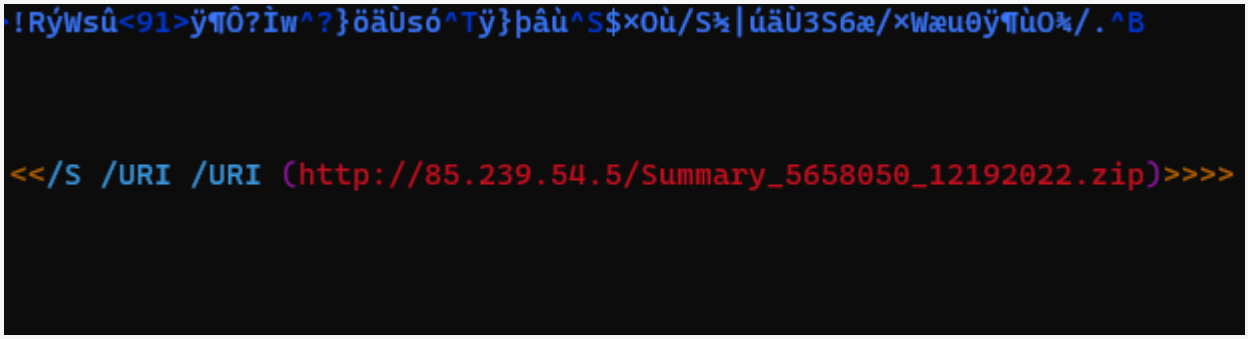


図2- クリックすると不正なアーカイブをダウンロードするPDFに埋め込まれたリンク

攻撃者のQRコードを使った機密情報を盗むための実験

2022年11月末、QRコードを悪用し、クレジットカード情報などの機密情報を盗み出す中国語の珍しいフィッシングキャンペーンを発見しました。[4] フィッシングやマルウェアのインシデントで使用される画像を比較する当社の内部分析システムにより発見されました。このキャンペーンでは、攻撃者はQRコードを使ってユーザーを悪意のあるWebサイトに誘導していました。

この攻撃は、Eメールで受信者に送信されるWordドキュメントから始まります。このドキュメントは、受信者が政府の助成金を受ける権利があるとするもので、権威への依存、緊急性、行動を起こすための金銭的動機付けといった、効果的なフィッシングルアーの典型的な要素に合致しています。

助成金を受け取るには、人気のインスタントメッセージ、ソーシャルメディア、モバイル決済アプリであるWeChatを使ってQRコードをスキャンし、その後はWebサイトの指示に従うことが求められます。

QRコードの使用は、フィッシング詐欺の防止や検知の仕組みが弱いPCからモバイル端末への切り替えを強制する効果的な方法です。また、QRコードはメールゲートウェイがコードの誘導先のWebアドレスを検査する可能性が低いため、通常のハイパーリンクに比べてフィッシングメールがユーザーの受信トレイに届く可能性が高くなるというメリットもあります。

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

10月末から、このようなフィッシングキャンペーンがほぼ毎日、高い頻度で観測されています。攻撃者は、毎日ドキュメントのルアーやドメインを変えています。これらのキャンペーンの規模について決定的なことは言えませんが、攻撃者が動的なフィッシングフレームワークを選択したことは、拡張性が考慮されたことを示しています。これらのキャンペーンが大量に配信されているのは妥当なところです。フィッシングキットの構造上、キャンペーンのコンテンツとテーマは容易に交換可能です。

また、宅配業者を装った英語でのフィッシングキャンペーンでQRコードが使用され、代金を請求されるケースも確認されており、個人および組織ともにこのようなキャンペーンに注意する必要があります。

図4 - 対象者のクレジットカード情報を要求するフィッシングサイト

偽ソフトウェアのマルバタイジングが増加中

新しいPCをセットアップするとき、多くの人はお気に入りのソフトウェアをインストールします。しかし、油断していると、お気に入りのソフトウェアを装ったマルウェアをインストールしてしまうかもしれません。昨年11月以降、不正な広告を利用して無防備な被害者にマルウェアを送りつけるキャンペーンが増加していることに我々は気づきました。[5]

マルバタイジングでは、悪意のあるアクターが検索エンジンの検索結果広告を購入し、ユーザーをマルウェアをホストするWebサイトにリダイレクトします。広告を購入することで、攻撃者はソフトウェア関連の検索に対して、悪意のあるWebサイトを検索エンジンランキングの上位に表示できます。我々が分析したいくつかの例では、攻撃者は、 Audacity、 Blender、GIMPなどの人気のあるオープンソースプロジェクトを模倣しています。これらのソフトウェアパッケージを検索したユーザは、悪意のあるWebサイトへ誘導する広告を表示される可能性があります。

図5は、偽のスポンサーリンクの例です。よく見ると、広告のドメイン名がソフトウェアプロジェクトの本物のWebサイトと異なっていることに気づくでしょう。しかし、ドメインの違いは微妙で、簡単に見逃してしまいます。広告をクリックすると、正規のAudacityのWebサイトのデザインをコピーした偽のWebサイトにつながります。

第4四半期のマルバタイジングキャンペーンで模倣されたソフトウェアプロジェクトの数

24

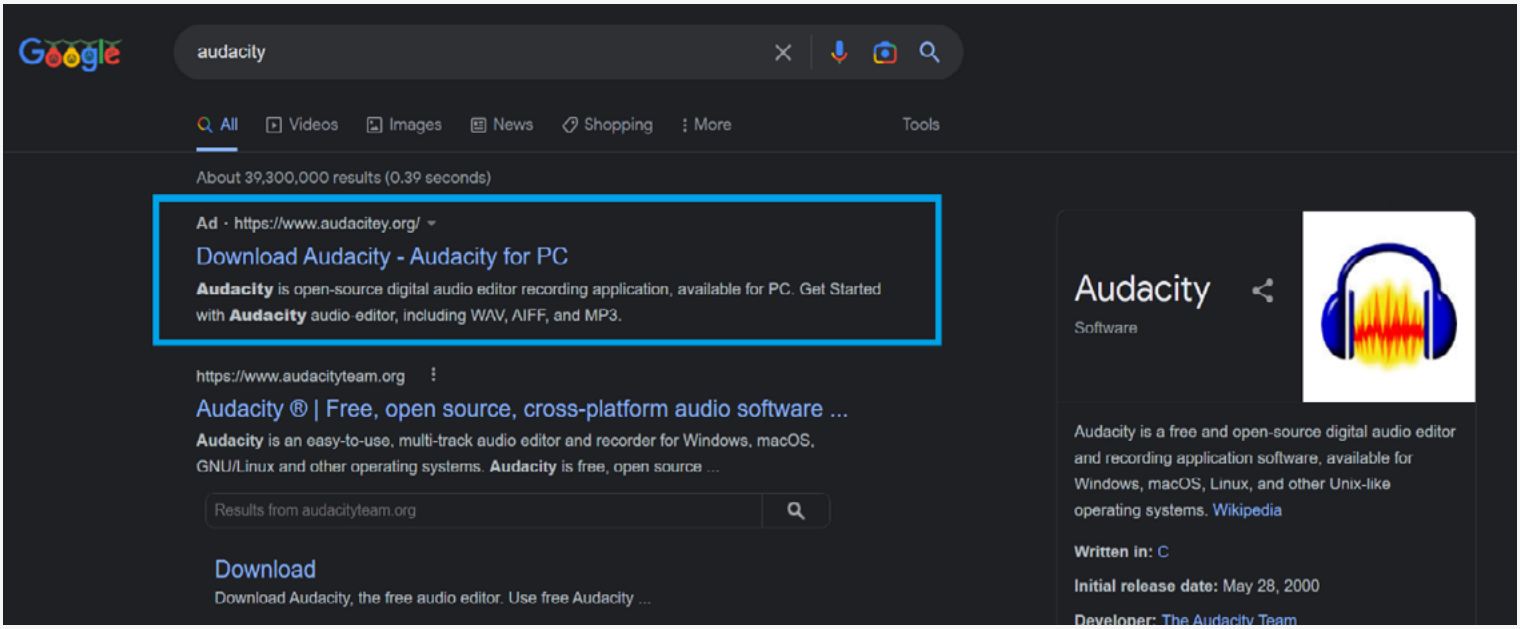


図5 - マルウェアを提供する悪意のあるWebサイトへ誘導する検索エンジン広告

偽のWebサイトは本物のWebサイトとほとんど同じように見えるため、ユーザーは偽のWebサイトであることを見破ることが困難です。（図6）ユーザーがダウンロードボタンをクリックすると、インストーラを装った.exeファイルが提供され、この場合には”audacity-win-x64.exe” が提供されます。この例では、商品情報を盗む Vidar Stealer が配信されました。[6] Vidar Stealerが、マルバタイジングによって配布されている唯一のファミリーというわけではありません。この偽ソフトウェアのマルバタイジングのテーマが、Rhadamanthys Stealer や BatLoader などのインフォスティーラーを含む、少なくとも8つのマルウェアファミリーの拡散に利用されていることも確認しています。[7][8]しかしながら、11月中旬以降、この配信方法を用いた最大のキャンペーンは、トロイの木馬 IcedID を拡散するものです。

Vidar Stealerと同様に、攻撃者はソフトウェアプロジェクトの正規のWebサイトを模倣してマルウェアを拡散します。攻撃者は、キャンペーンによってドメインのプロパティを変えない傾向があるため、ドメインレジストラ、ネームサーバー、ドメイン名に基づいて偽のWebサイトを特定することが可能です。

2ヶ月間の調査で、マルウェア配信に使用されたあるいは現在も使用されている可能性のある24種類のソフトウェアプロジェクトを模倣した92のドメインを特定しました。（図7および図8）脅威アクターがマルウェアの配信方法を多様化させる中、この傾向は今後も続くと予想されます。

図6 - Vidar Stealerを配信する偽AudacityのWebサイト

Domain	Registrar	Created	Name Server
wvw-irs-forms.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 29, 2022, 4:12 p.m.	a.dnspod.com c.dnspod.com
vvv-discord.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 29, 2022, 10:49 a.m.	a.dnspod.com c.dnspod.com
mlcrosofteams.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 29, 2022, 10:49 a.m.	a.dnspod.com c.dnspod.com
wvvw-citrix.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 28, 2022, 9:42 a.m.	a.dnspod.com c.dnspod.com
wvw-adobe.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 28, 2022, 9:42 a.m.	a.dnspod.com c.dnspod.com
vwvv-discord.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 28, 2022, 9:42 a.m.	a.dnspod.com c.dnspod.com
www-microsofteams.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 27, 2022, 1:44 p.m.	a.dnspod.com c.dnspod.com
vwv-discord.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 27, 2022, 1:44 p.m.	a.dnspod.com c.dnspod.com
www-onenote.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 26, 2022, 10:27 a.m.	a.dnspod.com c.dnspod.com
www-microsoftteams.top	NICENIC INTERNATIONAL GROUP CO., LIMITED	Dec. 26, 2022, 10:11 a.m.	a.dnspod.com c.dnspod.com

図7 - 2022年12月に登録されたタイポスクワットドメイン

Campaign date	Imitated software		Malware family
December 2021	Discord		Redline Stealer
February 2022	Windows 11 OS upgrade		Redline Stealer
November 2022 – ongoing	Audacity Blender GIMP Notepad++ Microsoft Teams Citrix Adobe OneNote LibreOffice Slack TeamViewer Any Desk	Thunderbird Fortinet Webex Sandboxie Plus Docker Basecamp VMWare OBS WhatsApp Tor Browser Crypto Browser Brave Browser	IcedID Vidar Stealer Rhadamanthys Stealer BatLoader Redline Stealer Aurora Stealer Gozi Raccoon Stealer

図8 - 偽ソフトウェアのマルバタイジングキャンペーンの要約

Emotetの配信者はOfficeの厳格なマクロポリシーを回避してPCを感染

第4四半期には、Emotetのキャンペーンはほとんど行われていませんでした。[9] しかし、11月2日から11日にかけて、このマルウェアは数ヶ月ぶりに新たなスパムキャンペーンを実施しました。このマルウェアは、Eメールに添付された悪意のあるマクロ対応のExcelスプレッドシートを介して、従来通り配布されました。しかし、そのドキュメントのデザインに変化が見られました。

長年にわたり攻撃者に悪用されてきたVisual Basic for Applicationのマクロは、2022年2月Microsoftによって、Webからダウンロードした多くのMicrosoft Officeファイルフォーマットでデフォルトで無効にされました。[10] この変更は、攻撃ファイルタイプの多様化という継続的なトレンドに寄与しています。興味深いことに、Emotetの配信者はマクロから離れるのではなく、単にポリシーを回避しようとしました。

図9 - 2022年11月のEmotetキャンペーンで使用されたソーシャルエンジニアリング画像

受信者がスプレッドシートを開くと、Officeのバナーを装ったソーシャルエンジニアリング画像が表示されます。ここにはスプレッドシートの内容を確認するには、表示されているフォルダのいずれかにファイルをコピーし、再度開く必要があると表示されています。HTMLスマグリングやPDFマルウェアの配信と同様、この方法は感染を引き起こすために高度なユーザー操作を必要とします。Officeのポリシーが変更される以前は、ユーザーの2回のクリックで不注意によるマルウェア実行をさせることができました。

ユーザがその指示に従うと、悪意のあるマクロが実行されます。このコードは、ユーザーのディレクトリに名前の異なるの4つのDLLファイルを保存し、regsvr32.exe (T1218.010) を使用してそれらを実行し、Emotetのペイロードを実行に至ります。[11] この複雑なユーザーの操作から、このキャンペーンは、この配信手法と他の方法との感染率の比較テストだった可能性もあります。

第3四半期にディスクイメージマルウェアが急増

31%

脅威の侵入経路

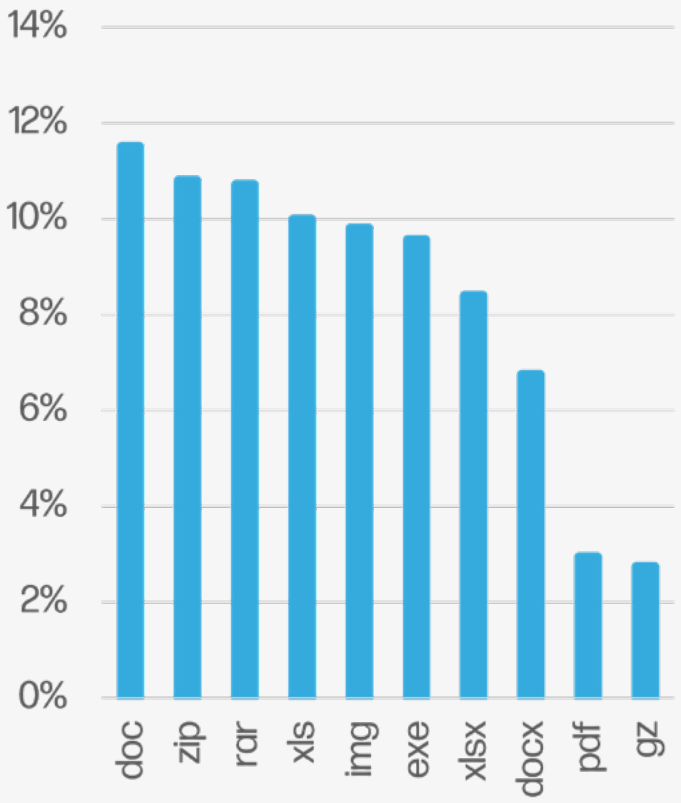
77%
Eメール

14%
Webブラウザーダウンロード

9%
その他

注目すべきトレンド

ファイルの拡張子



第3四半期からHTMLの脅威が増加

44%

3四半期連続でマルウェアの配信ファイルタイプとしてアーカイブが最多を継続

第4四半期には、マルウェアの42%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ています。アーカイブは、第3四半期もOfficeフォーマット（38%）を抑えて、最も人気のあるマルウェアのファイルフォーマットグループでした。脅威アクターがペイロードの実行にスクリプトを好むようになっているため、アーカイブの人気は2022年第1四半期から20%上昇しています。

マルウェアのファイル拡張子トップ10のうち4つがアーカイブフォーマット（ZIP、RAR、IMG、GZ）でした。特に、ディスクイメージ（IMG）マルウェアは、第3四半期と比較して31%増加し、第4四半期には、このフォーマットが2つ順位を上げて、最も人気のあるマルウェアのファイルタイプ第5位となりました。攻撃者は、Windowsの自動マウント機能を悪用し、ターゲットがIMGファイルをダブルクリックすることで簡単にマウントし、IMGファイル内に格納されているマルウェアにアクセスできるようにしています。

また、アーカイブの一種であるRARも3位にランクアップし、このファイルフォーマットを使用したマルウェアが11%確認されています。全体として、上位10種類のファイルフォーマットは、HP Wolf Securityが隔離・検知したマルウェアの83%を占めています。

アーカイブは簡単に暗号化でき、Webプロキシやサンドボックス、メールスキャナによるマルウェア検知が困難なため、脅威アクターにとって魅力的です。多くの組織が正当な理由で暗号化アーカイブを使用しているため、暗号化アーカイブのEメール添付をポリシーで拒否することは困難です。

第4四半期にHTMLの脅威が増加

HTMLスマグリングを含むHTMLの脅威は、第4四半期に44%増加し、15番目に人気のあるマルウェアフォーマットになりました。（第3四半期の17位から2ランクアップ）このテクニックがマルウェアを拡散するために脅威アクターの間で人気が高まっていることを示しています。

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。[12] [13]
- 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。[14]
- 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。[15] 最新の脅威に関する調査については、HP WOLF SECURITY ブログ [16] にアクセスしてください。

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://malpedia.caad.fkie.fraunhofer.de/details/win.icedid

[4] https://threatresearch.ext.hp.com/chinese-phishing-campaign-abuses-qr-codes-to-steal-credit-card-details/

[5] https://threatresearch.ext.hp.com/adverts-mimicking-popular-software-leads-to-malware/

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

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

[8] https://malpedia.caad.fkie.fraunhofer.de/details/win.bat_loader

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

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

[11] https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked

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

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

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

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

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

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。

© Copyright 2022 HP Development Company, L.P. ここに記載されている情報は、予告なく変更されることがあります。HP の製品およびサービスに関する唯一の保証は、当該製品およびサービスに付随する明示的な保証書に記載されています。本書のいかなる内容も、追加的な保証を構成することは一切ありません。 HP は、本書に含まれる技術的または編集上の誤りや脱落について責任を負いません。