HP WOLF SECURITY

脅威インサイトレポート

2023年第1四半期

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2023年第1四半期版へようこそ

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

14%

- 第1四半期OneNoteノートブックを通じてマルウェアを拡散し、Microsoft Officeの一部のファイルフォーマットのマクロ制限を回避する脅威が発生しました。この攻撃は被害者を騙して偽のUIをクリックさせ、悪意のあるスクリプトをダウンロードさせ、バックドアやリモートアクセス型トロイの木馬（RAT）にPCを感染させます。
- 3月、HP Wolf Securityは、悪意のあるGoogle Chrome拡張機能で被害者を感染させる新しいChromeLoaderマルウェアキャンペーンを検知しました。新しい亜種であるChromeLoader Shampooは、海賊版の映画やビデオゲームをホストするWebサイトを通じて配布されています。このマルウェアの機能には、検索クエリのリダイレクトやブラウジングセッションへの広告の挿入が含まれており、その運営者は金銭的な利益を得ることを目的としている可能性があります。
- マルウェアの配信手法やファイルタイプは、第1四半期も引き続き多様化しており、一部の悪質なスパム配信者は毎週ファイルタイプを変えています。HP Wolf Securityが確認したgzipとHTMLの脅威は、第1四半期に大幅に増加し、第4四半期比53%と37%増加しました。
- 攻撃者は、侵害されたMicrosoft 365アカウントを使用して同僚に悪意のあるEメールを送信することにより、Officeのマクロの制限を回避しようとしました。この攻撃者はハッキングフォーラムなどで販売されている、キー入力を記録し機密情報を盗むマルウェア・ファミリー FormbookにPCを感染させようとしました。

特筆すべき脅威

OneNoteが攻撃者に悪用されマルウェアを配信

1月、人手によるランサムウェア攻撃の一般的な前兆であるQakBotとIcedIDの配信者は、悪意のあるMicrosoft OneNoteノートブックを通じてマルウェアの拡散を開始しました。[2][3] OneNoteは人気のある無料のノート作成およびコラボレーションアプリケーションです。ファイル拡張子.oneで示されるそのファイルフォーマットは、多くの種類のマルチメディアを保存することができます。[4] ユーザーは、ノートブック内にコンテンツを簡単に埋め込むことができ、Eメールで他のユーザーと共有することができます。

残念なことに、攻撃者はOneNoteのコンテンツ埋め込み機能を悪用してマルウェアを拡散しています。Office、PDF、HTMLファイルが関与するマルウェアでよく見られるように、攻撃者は正規のプログラムプロンプトやUIのように見えるソーシャルエンジニアリング画像を利用して、被害者を騙してPC上で悪意のあるコードを実行させています。

第1四半期に確認されたOneNoteマルウェアのキャンペーンでは、ノートブック内のすべてのファイルを読み込むと思われるボタンをダブルクリックするよう求めるメッセージが表示されます。しかし、このボタンには、PCにマルウェアをダウンロードして感染させる悪意のあるスクリプトが潜んでいます。攻撃者は、検知を回避するために、Windowsスクリプトファイル（WSF）やHTMLアプリケーション（HTA）内のPowerShell、バッチ、JScriptなど、さまざまなスクリプト言語や難読化テクニックを使用しています。

第1四半期には、リモートアクセス型トロイの木馬やインフォスティーラーなどのコモディティ型マルウェアを拡散する攻撃者の間で、このマルウェア配信手法が流行しました。また、3月中旬に悪名高いクライムウェアファミリーEmotetの配信者が、OneNoteノートブックを利用した新たなスパムキャンペーンを展開し、一時的に復活しました。[5] しかしながらこのキャンペーンは長くは続かず、ボットネットは約2週間後に再び沈黙しました。

OneNoteノートブックは、攻撃者がマクロに依存することなく悪意あるコードを実行できるため、マルウェア拡散の手段として今後も使われる可能性があります。企業や個人は、この感染経路をブロックするための防御策を確認し実施する必要があります。例えば、社外からEメールでノートブックを受け取ることを想定していない場合、HP Sure Click Enterprise ポリシーを設定し、ユーザがリスクの高い外部ソースからのノートブックを信頼しないようにすることができます。[6]

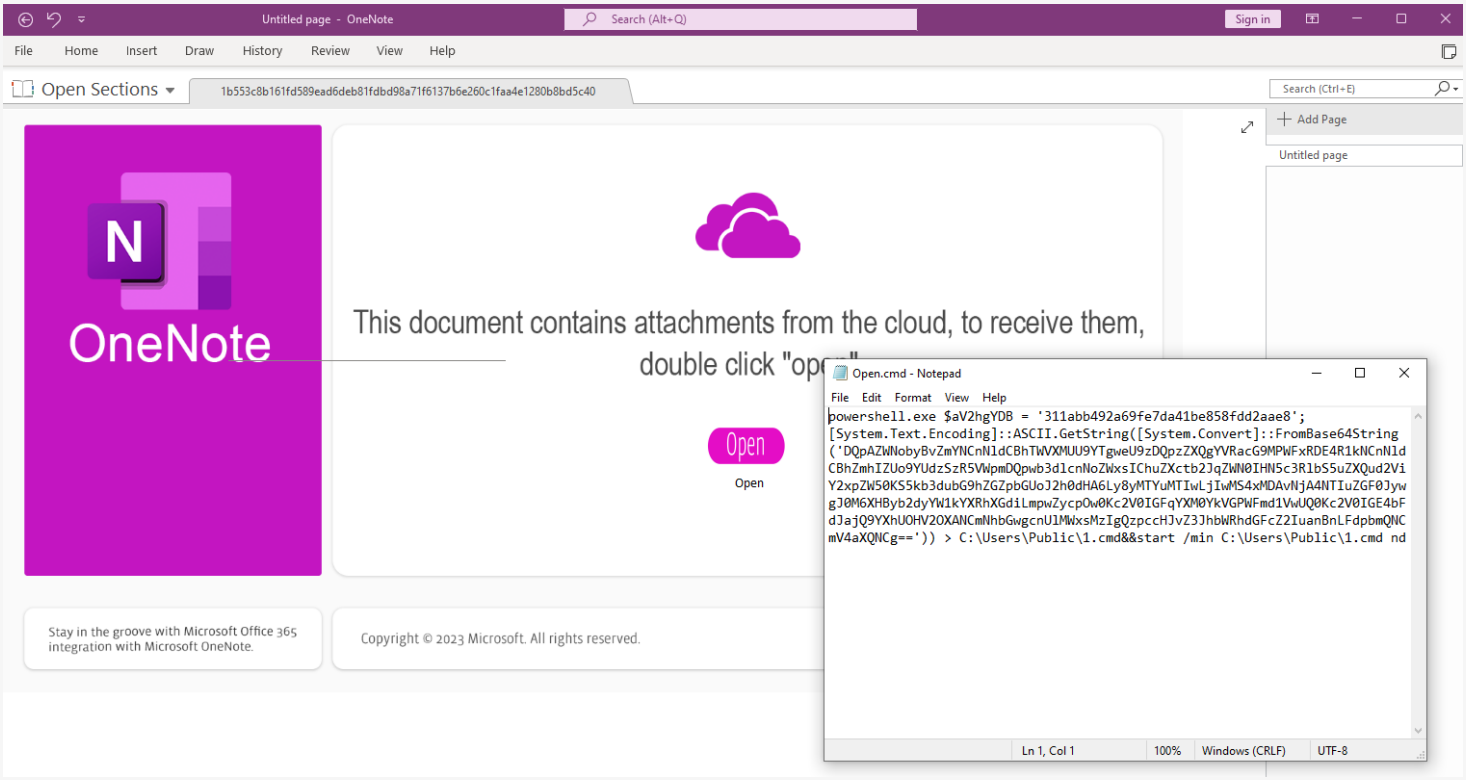


図1 - 悪意のあるバッチスクリプトを隠したOneNoteノートブック

海賊版コンテンツを求めるユーザーを感染させる新たなChromeLoaderキャンペーン

広告のブロックからパスワードの管理まで、ブラウザのエクステンションは私たちのWeb閲覧体験を向上させる強力なプログラムです。サイバー犯罪者は何十年もの間、Webブラウザの拡張性を悪用して金銭的な利益を得たり、個人情報を盗んだりしてきました。最初は不正なツールバーを通して、そして最近では怪しげなエクステンションを通して。[7]

3月、HP Wolf SecurityはShampooという悪意のあるGoogle Chromeエクステンションをダウンロードしようとするユーザーを検知しました。正規のエクステンションとは異なり、ShampooはChrome Web Storeでレビューされ公開されていません。その代わりに、被害者を騙して悪意のあるVBScriptを実行させることでPCに感染します。これにより一連のスクリプトが実行され、エクステンションがダウンロードされ、新しいブラウジングセッションにロードされ、削除を困難にする永続化メカニズムが設定されます。

Shampooは、2022年初頭にセキュリティ研究者によって初めて分析されたGoogle Chromeブラウザエクステンションマルウェアのファミリーであるの亜種です。[8] その目的は、Chromeに悪意のあるエクステンションをインストールし、検索クエリのリダイレクトや広告の挿入により、運営者に利益をもたらすことです。 ChromeLoader Shampooの感染経路は複雑で、海賊版の映画やビデオゲームなどの違法コンテンツをホストするWebサイトから、被害者が悪意のあるスクリプトをダウンロードすることから始まります。

被害者の多くは、Chromeが別のWebページにリダイレクトされたり、予期せず閉じたり開き直したり、ツールバーにアイコンが表示されることで、悪意のあるエクステンションに気づきます。しかし ChromeLoader Shampoo を削除するのは、正規のエクステンションほど簡単ではありません。ループするスクリプトとWindowsスケジュールタスクに基づき、被害者がエクステンションを削除したりデバイスを再起動したりするたびにエクステンションを再インストールします。

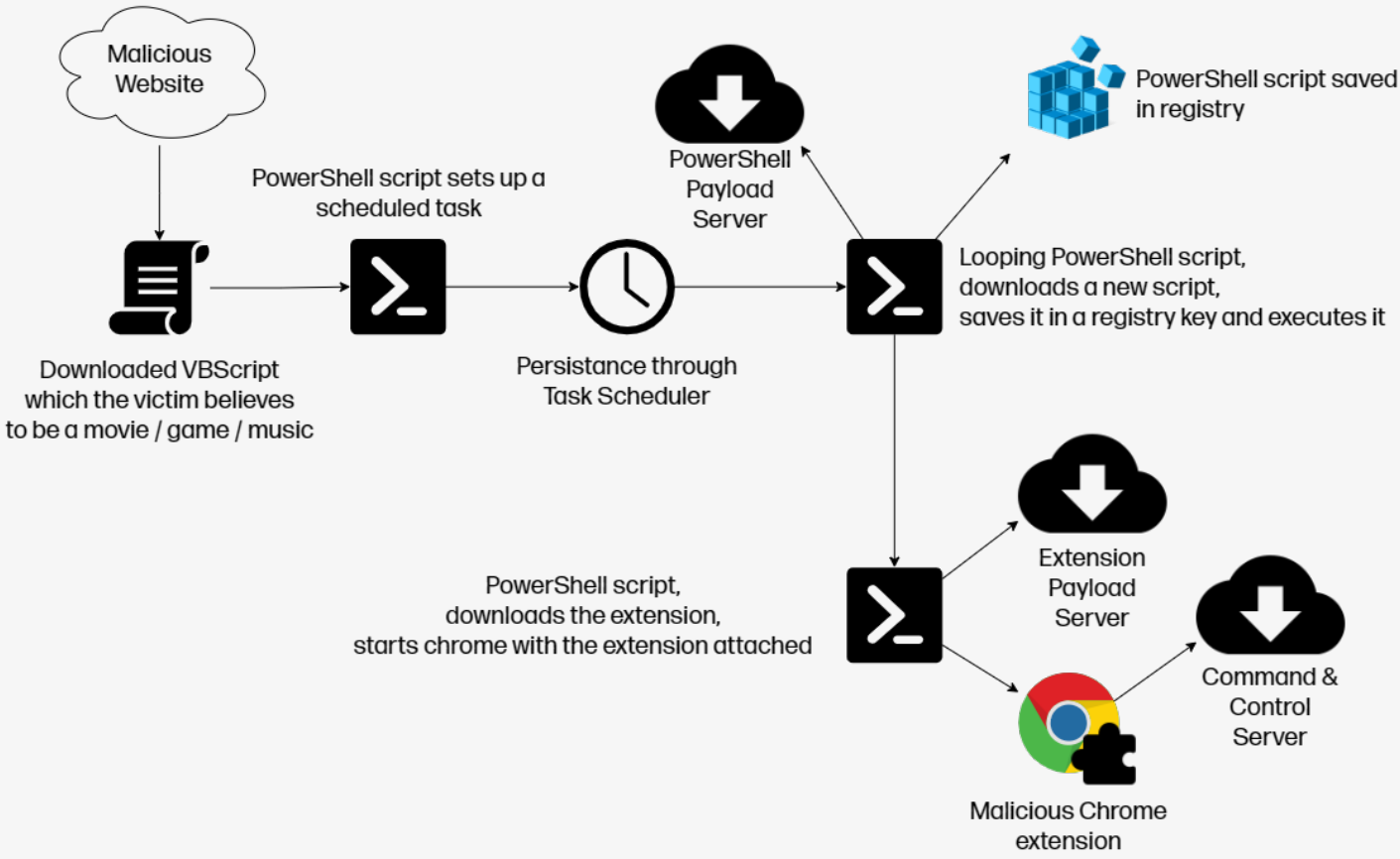


図2 - 2023年3月のChromeLoader感染チェーン

このキャンペーンの人的要素は注目に値します。マルウェアは自身を隠しません。被害者はほぼ確実にChromeLoaderの存在に気づきます。にもかかわらず、ユーザーはマルウェアを削除するためにIT部門に助けを求めることを躊躇する可能性があります。ChromeLoader は多くの場合、ユーザーが違法コンテンツをホストするWebサイトからダウンロードした悪意のある VBScript ファイルを通じて配信されます。ユーザーは、組織のIT利用ポリシーに違反したことによる影響を恐れているのかもしれません。

エンドポイントの可視性を高め、脅威について定期的にユーザを教育することで、積極的なセキュリティ文化を強化し、エクステンションのインストール可否の管理を徹底することは、悪意のあるブラウザエクステンション を軽減するための実用的な手段です。 HP Sure Click EnterpriseのSecure Browser を使用すると、IT チームは、一元管理されたポリシーによって、不明または未承認のエクステンションのインストールをブロックできます。[9]

ChromeLoader Shampooを駆除するには、その永続化メカニズムを無効にする必要があります：

- 先頭に "chrome_"が付いたスケジュールタスク。正規のChromeスケジュールタスクは通常、"Google "が先頭に付きます。
- レジストリキーは"HKCU:\Software\Mirage Utilities\"。
- ループするスクリプト。これは、マシンを再起動することで一時的に無効になります。

これらの削除手順は、ループするスクリプトがマルウェアを再インストールする前に素早く完了させる必要があります。

Shampoo、または他のChromeLoaderの亜種がマシン上に存在するかどうかを検知する簡単な方法は、Chromeが"--load-extension"引数で実行されているかどうかを確認することです。ChromeLoaderはこの引数を頼りに、Chromeセッションにエクステンションをロードします。

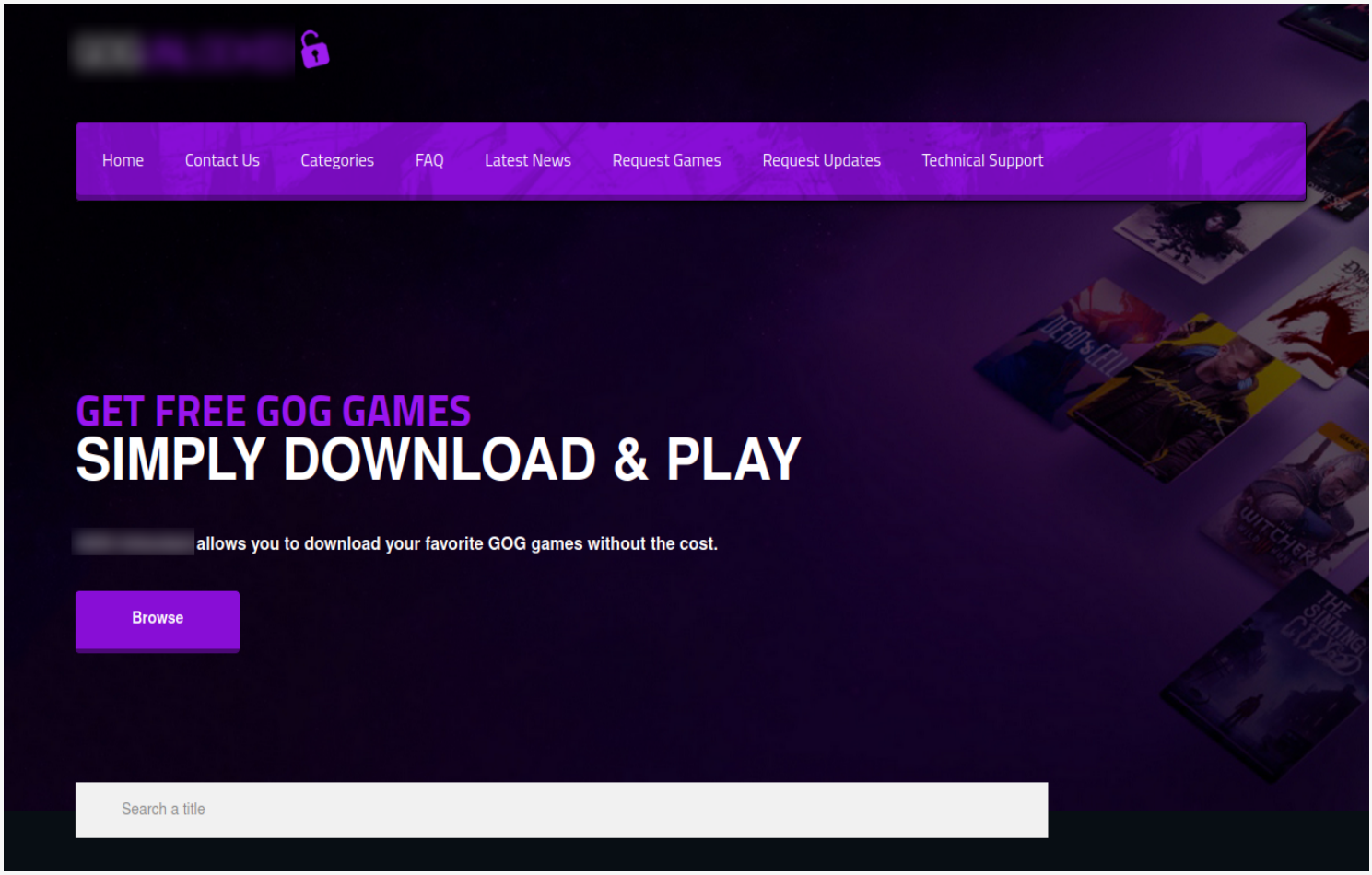


図3 - Shampooマルウェアを配布するWebサイト

攻撃者が信頼できるドメインを悪用してFormbookを配信

MicrosoftがOfficeのデフォルトセキュリティポリシーを強化した結果、脅威アクターは攻撃手法を変更し多様化させています。[10] VBAマクロは、Webなどの信頼できないソースからダウンロードされたドキュメントでは、デフォルトで無効になりました。しかし、3月初めに見られたキャンペーンでは、一部の攻撃者がこの制限を巧みに回避しています。

攻撃者はまず、従業員のMicrosoft 365の認証情報にアクセスしました。次に、この認証情報を使ってOutlook for Webにログインし、標的組織の財務部門を装った新しいEメールアドレスを設定しました。侵入を拡大するために、攻撃者は組織内の他の従業員の内部配布リストに悪意のあるWordドキュメントをEメールで送信しました。

このEメールが外部の送信者から発信されていれば、攻撃は成功しなかったでしょう。しかし、同じドメイン内で送信されたため、ドキュメントはOfficeによって信頼できるとみなされ、VBAマクロは無効化されませんでした。送信者が同僚の従業員であったため、悪意のあるEメールはより信頼性が高く見え、疑惑の目を向けられる可能性は低くなりました。

悪意のあるドキュメントのVBAマクロは単純で、データ転送ツールcurl.exeを使用して、URLからマルウェアのペイロードをダウンロードして実行するものでした。ダウンロードされたマルウェアはハッキングフォーラムで販売されているインフォスティーラーFormbookで、キー入力を記録し、機密情報を窃取することができます。[11]

このケースは、ドメインによりファイルを自動的に信頼することが、脅威アクターがターゲット環境内のアカウントをすでに侵害した攻撃には、対応できないということを浮き彫りにしています。最小権限の原則をエンドポイントから受信したファイルにも適用する（ゼロトラストのアプローチ）ことで、ユーザーを二次感染から守ることができたはずです。

Received From	emp1@domain.com <emp1@domain.com>
Sent To	emp2@domain.com <emp2@domain.com>
Date Sent	March 6, 2023 11:11 AM
Subject	FW: PI -0145
Attachments	pi-0147.docm (20KB) Script-Macro.Trojan.Heuristic

図4 -（個人情報を削除済みの）Formbookを社内の配布リストを通じて広めようとするEメール

脅威の侵入経路

80%
Eメール

13%
Webブラウザーダウンロード

7%
その他

第4四半期にgzipアーカイブマルウェアが増加

53%

注目すべきトレンド

多様化するマルウェア配信ファイルの種類と手法

第1四半期は、攻撃者がマルウェアを配信する際に使用するファイル タイプや手法が引き続き多様化しましたが、これは2022 年第1四半期以降、継続的に見られる傾向の一端です。特に、IcedID、Qakbot、Ursnifの配信手法は、旧来のキャンペーン活動と比較して大きく変化しています。[12] 2022年、マルウェアの配信手法には確実な変化が見られました。例えば、6月にQakbotの配信者がHTMLスマグリング（T1027.006）[13]に切り替えました。その後、12月には攻撃者はスパムキャンペーンで悪意のあるリンクを含むPDFドキュメントの送信を開始しました。そして2023年1月には、悪意のあるスクリプトを含むOneNoteノートブックへの移行が見られました。

しかしながら、それだけにとどまりませんでした。この3ヶ月間、攻撃者はこれらのテクニックを交互に使っています。ある週にPDFのルアーが送信されると、次の週にはHTMLスマグリングキャンペーンが行われることもありました。このようなスイッチは、攻撃者が主にWordドキュメントやExcelスプレッドシートなど、一握りのOfficeフォーマットに依存してマルウェアを配信していた過去のキャンペーンとは異なります。

攻撃者は、さまざまな種類のファイルを使用する以外にも、Eメール以外の感染経路を探求しています。2022年第4四半期に指摘された、攻撃者が検索エンジンの広告を利用して、マルウェアをホストする偽ソフトウェアプロジェクトのWebサイトに被害者を誘い込むマルバタイジングの流行は現在も続いています。[14]

第4四半期にHTMLの脅威が増加

37%

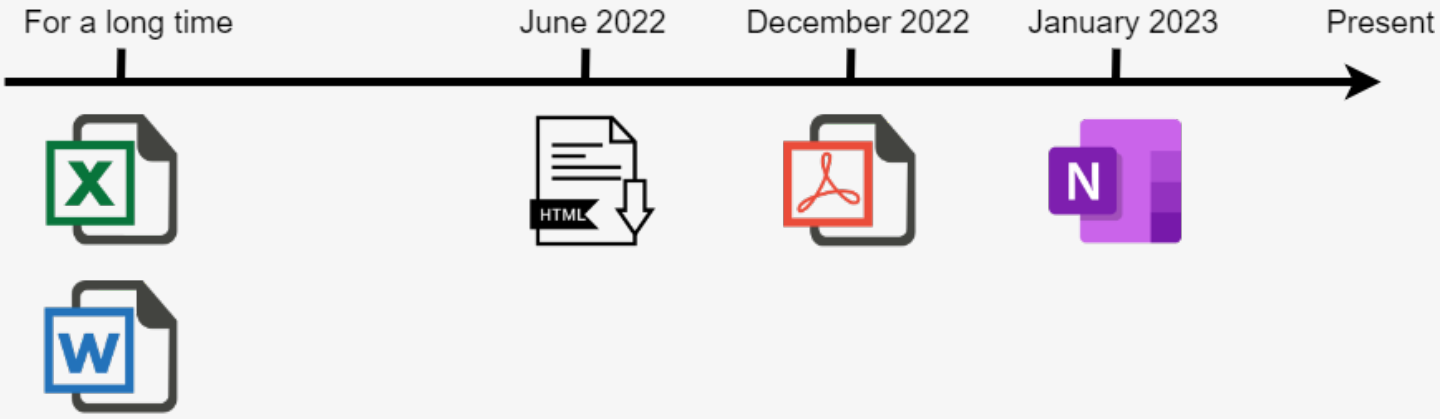
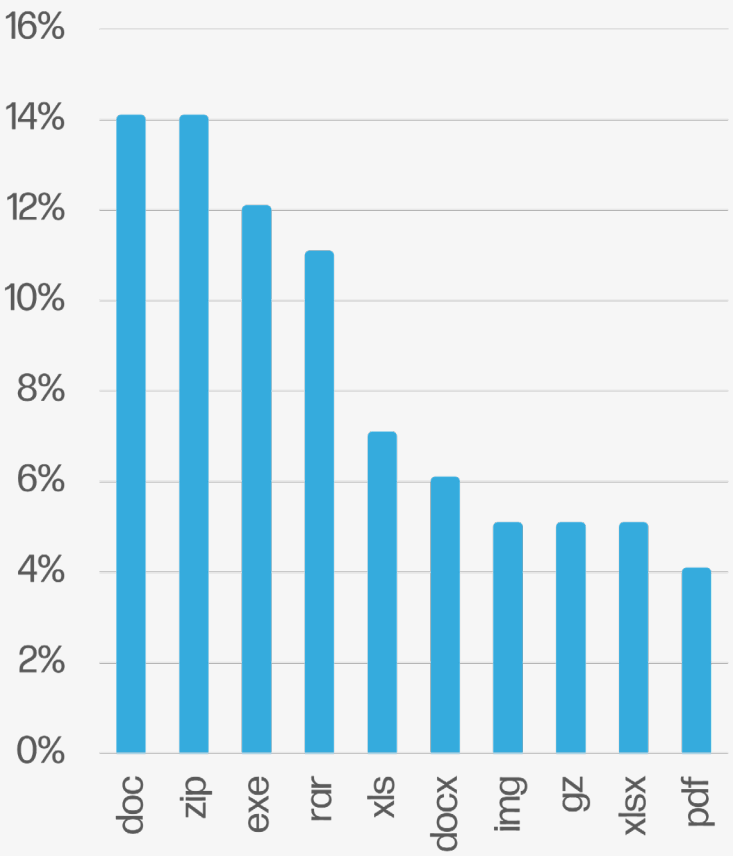


図5 - 2022年から2023年初頭にかけてのQakBot配信テクニックのタイムライン

マルウェアのファイル拡張子



脅威のファイルタイプのトレンド

アーカイブは、第４四半期も引き続き最もよく利用されたマルウェア配信ファイルタイプで、第１四半期の脅威は第４四半期と比較して２ポイント増加しました。特に、Remcos、Agent Tesla、Ave Mariaのようなを配信する注文書不正スパムによって、gzip（.gz）形式のアーカイブ型マルウェアが前期比で53%増加しました。[15][16][17] gzipファイルにはWindowsのデフォルトのファイルハンドラがないため、攻撃者はユーザーが7-Zipのようなファイルアーカイバをインストールしマルウェアを展開することに依存していると考えられます。HP Wolf Security が確認した Zip アーカイブの脅威も、第１四半期に 8% 増加しています。

スプレッドシートマルウェアは、第4四半期と比較して、第1四半期は19%から13%へと6ポイント減少しました。これは攻撃者がOfficeフォーマットから離れたためです。現在、Officeの脅威のほとんどは、マクロではなく、コード実行を目的としたエクスプロイトに基づいています。第1四半期にHP Wolf Securityが阻止したWordの脅威の85%は、悪意のあるマクロではなく、CVE-2017-11882などのエクスプロイトに基づいていました。[18] 同様に、HP Wolf Securityが阻止したExcelの脅威の62%にはエクスプロイトが含まれていました。

HTMLスマグリングを含むHTMLの脅威は増加し続けています。第1四半期は、HP Wolf Securityが阻止したこのファイルタイプの脅威が、第4四半期と比較して37%増加しました。

第1四半期のエクスプロトを含むドキュメント脅威

85%

脅威の侵入経路

エンドポイントに脅威を送り込む経路として、依然としてEメールが上位を占めています。HP Wolf Securityが第1四半期に確認した脅威の80%はEメールによるもので、第4四半期と比較して3ポイント増加していました。

Eメールセキュリティをバイパスしたメール脅威の数も第1四半期に増加しました。HP Wolf Securityが検知したEメール脅威の14%は、1つ以上のEメールゲートウェイスキャナーをバイパスしており、前四半期より1ポイント増加しました。

悪意のあるWebブラウザーダウンロードは、第1四半期に1ポイント微減して13%となりました。リムーバブルメディアなど、その他の経路による脅威は、第4四半期に比べて2ポイント減少し7%となりました。

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。[19] [20]
- 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。[21]
- 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。[22] 最新の脅威に関する調査については、HP WOLF SECURITY ブログ [23] 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://learn.microsoft.com/en-us/openspecs/office_file_formats/ms-one/73d22548-a613-4350-8c23-07d15576be50

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

[6] https://www.hp.com/us-en/security/products.html#section=SureClickEnterprise

[7] https://www.malwarebytes.com/blog/threats/toolbars

[8] https://www.gdatasoftware.com/blog/2022/01/37236-qr-codes-on-twitter-deliver-malicious-chrome-extension

[9] https://enterprisesecurity.hp.com/s/article/Using-Browsers-with-vSentry

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

[11] https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

[12] https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi

[13] https://attack.mitre.org/techniques/T1027/006/

[14] https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-q4-2022/

[15] https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos

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

[17] https://malpedia.caad.fkie.fraunhofer.de/details/win.ave_maria

[18] https://nvd.nist.gov/vuln/detail/cve-2017-11882

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

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

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

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

[23] 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. H 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。