HP WOLF SECURITY
脅威インサイト レポート

1H - 2021

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2021年1H版へようこそ。ここでは、HP Wolf Securityのセキュリティエキスパートが、2021年上半期に**HP Wolf Security**が特定したマルウェアの傾向を紹介し、セキュリティチームが新たな脅威に対抗し、セキュリティの状態を改善するための知識を身につけられるようにします。[1]

マルウェアを使った攻撃の多くは金銭的な動機に基づいています。脅威アクターは、自分のアクセスを収益化するための最短ルートを探しています。インフォスティーラー（情報窃盗型マルウェア）やリモートアクセス型トロイの木馬（RAT）の場合は、被害者のコンピュータに保存されている情報を売ることが一般的です。 しかし最近では、特に感染したシステムがActive Directoryドメインに接続されている場合は、システムがラテラルムーブ（横展開）が可能な大規模ネットワークの一部であることを示しているので、攻撃者は自分のアクセス権を他の脅威アクターに売却することも増えています。

サイバー犯罪者の不正アクセスに対する要求は、ランサムウェアのアフィリエイトがネットワークへの侵入口を必要としていることにより、非常に高まっています。また、通信手段や追跡困難な暗号通貨などの技術向上により、組織犯罪として直接的に、あるいは不正な商品やサービスの取引によって間接的に、脅威アクター同士が協力し合うことが容易になっています。その結果、資金力の乏しい脅威アクターが販売した不正アクセスが、資金力と経験豊富なランサムウェア・アズ・ア・サービス（RaaS）のアフィリエイトの手に渡ってしまう可能性があります。このように、1つのシステムへの最初の侵害が、事業継続に大きな影響を与えるインシデントへと発展してしまいます。

特筆すべき脅威

増加するハッキングツール

2021年上半期のHP Wolf Securityのテレメトリーでは、2020年下半期と比較して、ファイル共有サイトやアンダーグラウンドフォーラムからダウンロードされたハッキングツールが65%増加しています。さまざまなタイプの脅威がもたらすリスクを評価する一つの方法は、欲望、期待、知識、リソースなどの脅威アクターを駆り立て、犯罪を可能にする要因を検討することです。ハッキングツールの使用数の増加は、攻撃者の意図、すなわち攻撃を実行したいという欲求とそれが成功するだろうという期待の増加を示していると考えられます。また、サイバー犯罪のエコシステムの中でハッキングツールが広く利用されていること、すなわち攻撃者が自由に使えるリソースがあることを示しています。ハッキングツールが簡単に手に入るようになった背景には、マルウェアの海賊版や「クラッキング」が蔓延し、開発者が意図していなくても、誰もが無償でツールを使用できるようになっていることがあります。

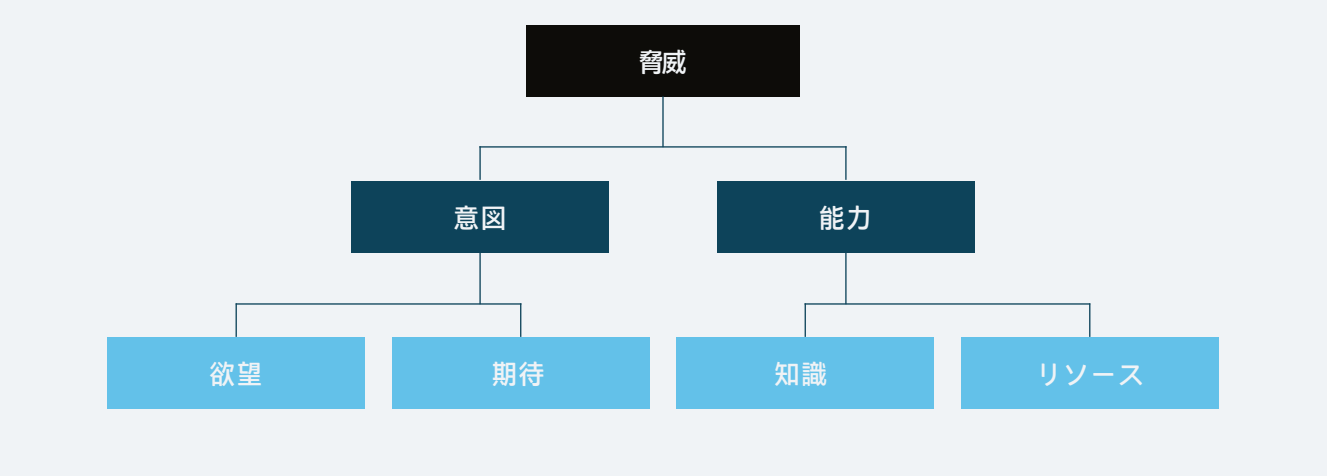


図 1 – 脅威の主要ドライバー

知識の共有も、我々のハッキングツールの脅威評価に繰り入れます。アンダーグラウンドのフォーラムやチャットルームは、脅威アクターが戦術、技術、手順（TTP）を共有したり、盗んだデータや不正アクセスを売買したりするための理想的なプラットフォームとなっています。例えば、3月にHP Wolf Securityは、トルコ語のクラッキング・フォーラムから**Sentry MBA**のクラッキング・コピーをダウンロードするユーザーを検知しました。この人気の高いハッキングツールは、**クルデンシャル・スタッフィング（パスワードリスト型攻撃）** - 攻撃者が漏洩した認証情報のリストを使ってウェブサイトの認証を試みる手法 - を行うために使用されます。[2] Sentry MBAの機能には、CAPTCHAチャレンジやWebアプリケーション・ファイアウォールなど、Webサイトのセキュリティ対策を回避する機能が含まれています。攻撃者は、あらかじめバンドルされている光学文字認識（OCR）のコンピュータ・ビジョン・モデルを使用するか、攻撃中にサードパーティのCAPTCHA解決サービスのAPIを照会するようにツールを設定することができます。

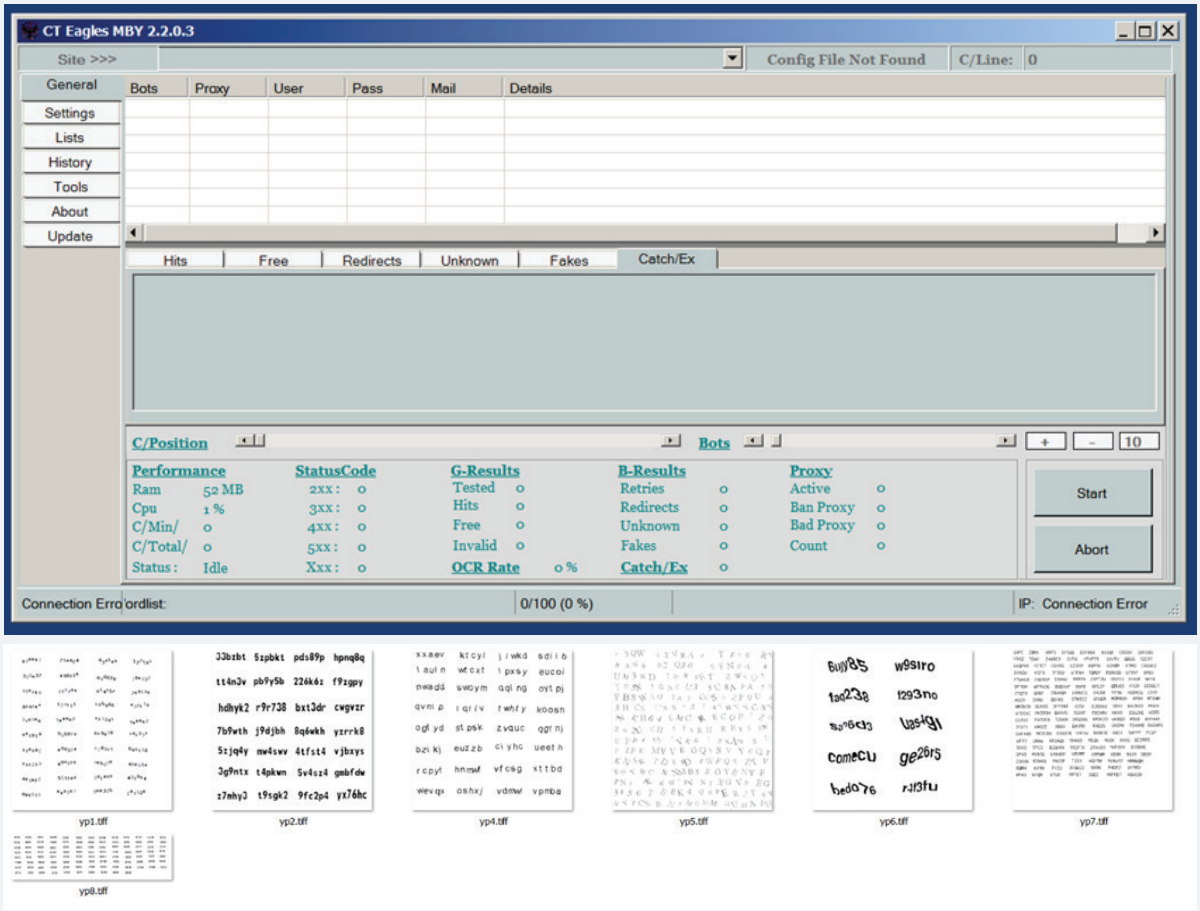


図2 & 3 – クラッキングフォーラムからダウンロードしたSentry MBA クルデンシャル・スタッフィング・ツールとCAPTCHAの文字セットのクラッキングコピー

2021年7月の時点で、特定のウェブサイトやデバイスに対してSentry MBAを使用するための設定やヒントを共有するための活発なフォーラムが多数存在しており、このようなツールの人気と、この種のサイバー犯罪への参入障壁の低さを示しています。

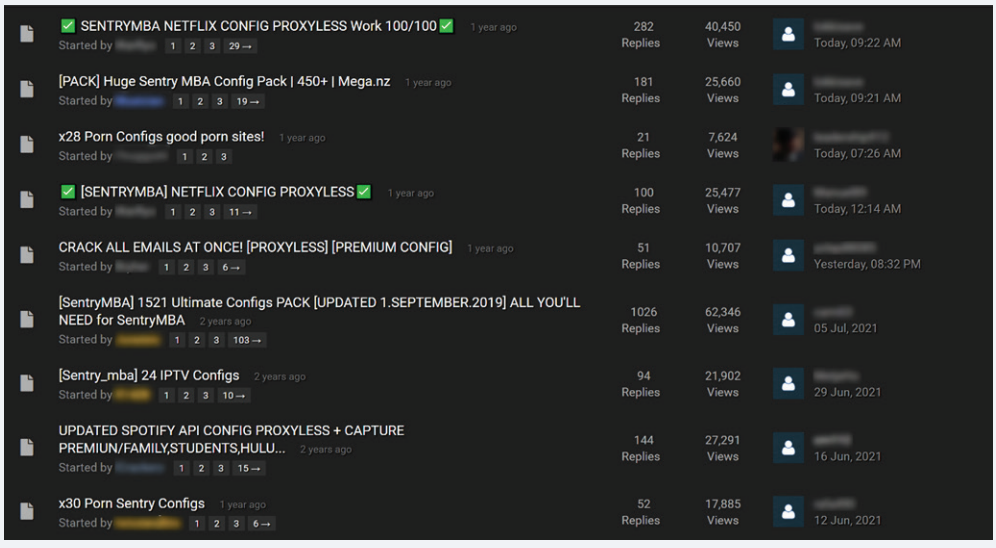


図4 – 2021年7月のSentry MBAの設定を共有するフォーラムの英語セクション

エグゼクティブを標的にしたマルチステージ・ダウンローダー

2021年3月、HP Wolf Securityは、エグゼクティブを標的にしたマルチステージのVisual Basic Script（VBS）マルウェア・キャンペーンを隔離しました。ターゲットは、姓と名の入った電子メールで悪意のあるZIP添付ファイルを受け取ります。名前と電子メールアドレスは、オンラインで公開されている情報から入手したものと思われます。この添付ファイルには、難読化されたVBSダウンローダーが含まれており、リモートサーバからユーザの%TEMP%フォルダに2つ目のVBSスクリプトをダウンロードします。第一ステージのスクリプトは高度に難読化されており、検知率が低く、VirusTotalに掲載されているアンチウイルススキャナのうち、21%しか悪意のあるものとして検知しませんでした。

第2ステージは、Windowsに組み込まれた正規のfile転送ツールである**BITSAdmin**を使ってダウンロードされます。脅威アクターは一般的に、**live off the land（環境寄生型）**と呼ばれる戦術を採用しており、OSの管理ツールや機能を利用して悪意のある行為を行い、検知の可能性を低くしています。このスクリプトは、システム上での永続性を確立するために、Windows Script Host（cscript.exe）でfileを実行するスケジュールタスクを作成します。

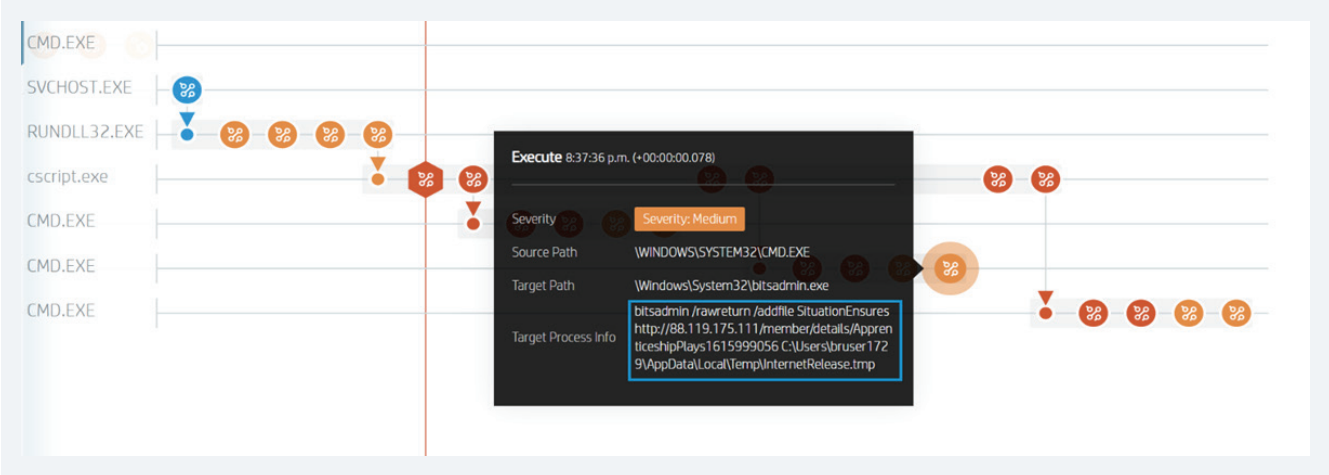


図 5 – HP Wolf Security ControllerがBITSAdminダウンロードコマンドを表示している隔離されたVBSダウンローダのサンプル

第2ステージでは、BITSAdminを使用して3つ目の難読化されたVBSファイルを%LOCALAPPDATA%Tempにダウンロードします。ダウンロードされたファイルのサイズに応じて、第3ステージでは、VBSファイルまたはポータブル実行ファイル（おそらく最終的なペイロード）として実行されます。攻撃者のコマンド＆コントロール（C2）インフラストラクチャは、解析時に第3ステージを活発には展開していなかったため、どのようなマルウェアが配信されるかを確認することはできませんでした。

Remcosを配信する履歴書をテーマにしたフィッシング・キャンペーンが企業を標的

2021年1月、HP Wolf Securityは、7カ国（チリ、イタリア、日本、パキスタン、フィリピン、英国、米国）の企業を対象とした悪質なスパムキャンペーンを隔離しました。就職希望者からのメールを装い、Microsoft OfficeのEquation Editorの脆弱性である**CVE-2017-11882**を悪用した悪意のあるRTF（Rich Text Format）ドキュメントが含まれていました。エクスプロイトに成功すると、このドキュメントは感染したシステム上に**Remcos**をダウンロードして実行しました。[3] 脅威アクターは、ダイナミックDNSサービス（gotdns[.]ch）のサブドメインをC2サーバーとして使用しました。Remcosは、感染したコンピュータにバックドアアクセスを与える市販のRATです。

標的となった業界:

- **製造**
- **海運**
- **商品取引**
- **海事産業**
- **不動産**
- **工業用品**

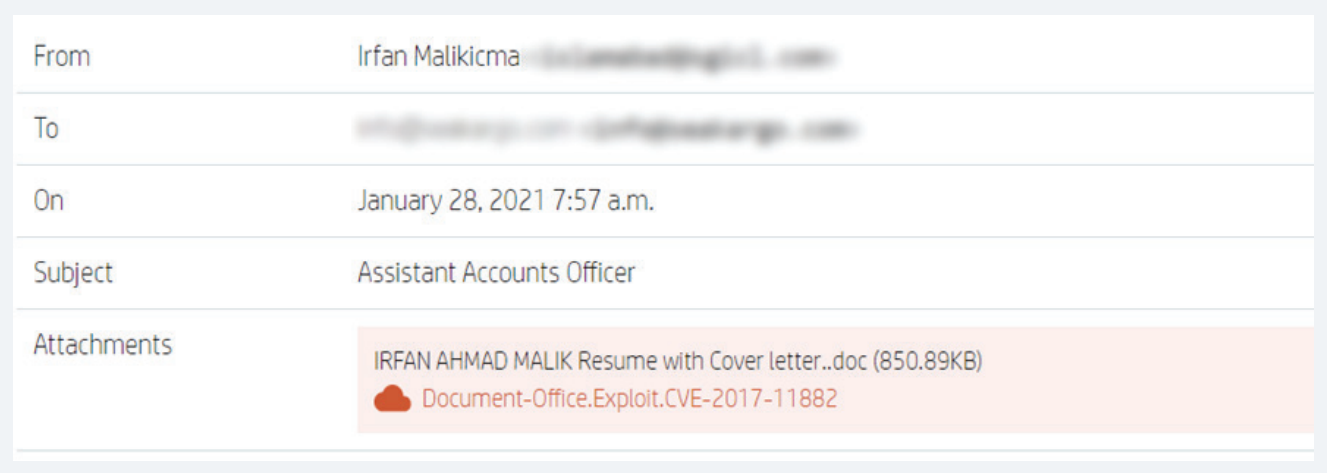


図6 – 求職者を装った悪意のあるEメール

DanaBotの配布に使われたCryptBot（クリプトボット）

2021年5月、HP Wolf Securityは、システムやWebブラウザの認証情報や暗号通貨ウォレットを収集する情報収集型 **CryptBot** を配信するキャンペーンを検知しました。CryptBotは、インフォスティーラーとして使用されるのではなく、後続のバンキング型トロイの木馬 **DanaBot** をドロップするために使用されました。DanaBotは、金融犯罪グループ **TA547** に関連するマルウェアの一種です。[4] 脅威アクターは、情報収集型ハッキングツールを使って他のマルウェアを展開するなど、必ずしも開発当初ではない目的に使用することで、マルウェアやその他のツールを日常的に再利用しています。

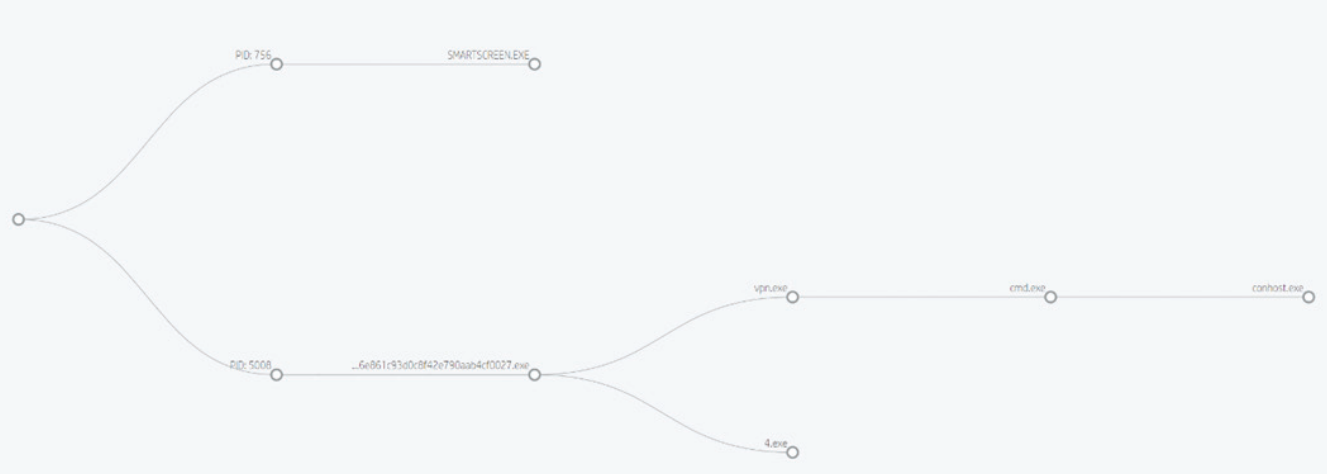


図7 – HP Wolf Securityマイクロ VM内で安全に、CryptBotがDanaBotをダウンロードし実行しているプロセスインタラクショングラフ

汎用的インフォスティーラー型マルウェアでコードの再利用が多発

Snakeは、2020年11月下旬に初めて発見されたモジュール型の.NETキーロガーおよびクレデンシャルスティーラーです。2021年上半期、HP Threat Researchチームは、このマルウェアファミリーをRTFやアーカイブ添付ファイルで配布する悪質なスパムキャンペーンを定期的に確認しています。Snakeのコードを分析したところ、過去2年間に活動していた他の4つのキーロガー・ファミリーとの間に類似点があることが判明しました。[5] 既存のマルウェア・ファミリーのソースコードを日和見的にコピーするというこの「リミックス」行動は、サイバー犯罪者が独自のマルウェア・アズ・ア・サービス・ビジネスを作ることがいかに容易であるかを示すものであり、企業の防御がマルウェア開発者の先を行くことの重要性を示しています。

図8 – SnakeキーロガーとMatiexキーロガーのキーストローク抽出関数の比較

Purple FoxがCVE-2021-26411をエクスプロイトしInternet Explorerユーザーを危険にさらす

HP Wolf Securityのテレメトリーで、ユーザーが遭遇した**Purple Fox**エクスプロイトキット（EK）の隔離されたサンプル数が増加していることがわかりました。

2021年4月に行われたあるキャンペーンでは、顧客のウェブブラウザのセッションがマイクロVM内で実行されていたために、HP Wolf Securityが、顧客の情報漏洩を防ぎました。[6] このサンプルでは、Purple Foxが新たに追加したInternet Explorerのメモリ破壊の脆弱性（**CVE-2021-26411**）を悪用しようとしていました。[7] このエクスプロイトのコードは、2021年3月中旬に公開された概念実証（PoC）に類似していました。PoCから実際の観測までの期間は数週間だったため、組織はPurple Foxに侵害されるリスクを負う前に、パッチを当てるわずかな時間しかありませんでした。

*図9 - CVE-2021-26411の経緯を示すタイムライン*か

ユーザーがPurple Foxに遭遇したのは、以下の用語を検索した後です。"قرايز-ديدمت-جذومن -"（アラビア語で "Form-extension-visit-"）ユーザーが、検索結果（loislandgraf[. us)をクリックすると、いくつのリダイレクトを経由してエクスプロイトを配信しようとするWebページに誘導されました。分析の過程で、すべてのケースでエクスプロイトが起動しなかったことに気づきました。これは、ジオフェンシングを使用して、どのシステムを侵害するを制御していたためと考えられます。イタリア、スイス、アイルランド、スウェーデン、日本が、感染チェーンを引き起こした国として挙げられていますが、これは網羅的なリストではありません。

注目すべきトレンド

アーカイブは現在最も人気のあるマルウェア配信ファイルタイプ

2021年上半期のマルウェア配信のファイルタイプは、アーカイブがトップで、2020年下半期からドキュメントを上回っています。この増加は、攻撃者がメールの添付ファイルでマルウェアを配信する際に、悪意のあるJava Archive file（.JAR）に切り替えたことが一因となっています。JARファイルを開くと、JAVAランタイム環境がインストールされている場合には、被害者のPC上でペイロードが解凍されて実行されます。私たちが目にした最も一般的なペイロードは、**AdWind**などのアンダーグラウンド・マーケットプレイスで簡単に購入あるいは入手できる低コストのRATでした。

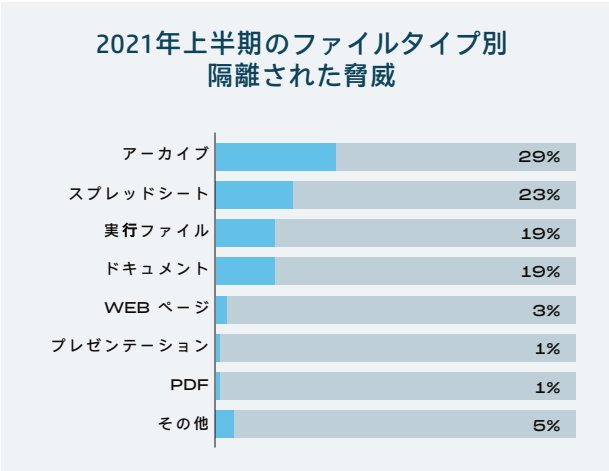


図10 – 2021年上半期のファイルタイプ別 Wolf Securityが隔離した脅威

これらのキャンペーンでは、発注書、請求書、製品仕様書、見積依頼書、品質管理報告書などのメールが上位を占めており、攻撃者が個人ではなく企業をターゲットにしていることがうかがえます。

また、.Z、.ARJ、.XZなど、通常とは異なる形式のアーカイブを利用して、汎用マルウェアを配信する攻撃も継続的に確認されています。攻撃者が特殊なファイルタイプを好む理由の1つは、メールゲートウェイのスキャナが、一般的でないフォーマットを使用したファイルを解凍して検査することができないため、悪意のあるメールがターゲットの受信箱に届く可能性が高くなることです。

マルウェアの配信に使用されたファイルタイプとしては、Excelのスプレッドシートが2番目に多く使用されました。これは、**Dridex**、**IcedID**、**TrickBot**などのクライムウェアを配布する大規模な悪意のあるスパムキャンペーンによるものです。また、Excelのスプレッドシートを利用して**Formbook**のような汎用スティーラーを配布する攻撃者も見られましたが、その規模ははるかに小さいものでした。HP Wolf Securityのデータによると、クライムウェアのアクターは、マルウェアの配布にスプレッドシートを使用することを好み、小規模で組織化されていないアクターは、アーカイブの利用を好むようです。

2020年下半期と比較して、HP Wolf Securityのテレメトリーでは、Webブラウザを使用してダウンロードされた脅威が24%増加しました。これは、ユーザーがハッキングツールや暗号通貨のマイニングソフトウェアをダウンロードしたことが一部要因となっています。Eメールは依然としてトップの感染経路であり、2021年上半期にHP Wolf Securityが隔離した脅威の75%はEメールで配信されました。2021年上半期、脅威の約3分の1（34%）は、検知時にアンチウイルスによるスキャンのハッシュが不明であり、2020年下半期から4%減少しました。

2021年上半期に hp wolf security が隔離された脅威の中で、

75%

がEメールで配信されていました。残りの 25% は Web ダウンロードでした。

COVID-19 Eメールルアーの人気がなくなる

HP Wolf Securityによって隔離された悪意のあるEメールに使用されたルアーの約半数（49%）は、ビジネス取引をテーマにしていました。これは、サイバー犯罪者の組織化が進んでいる一方で、ユーザーは相変わらず同じ手口に引っかかり、危険なファイルをダウンロードしたり、悪意のある添付ファイルや危険なWebリンクをクリックしたりしていることを示しています。

COVID-19をルアーとして使用したメールは、隔離されたメールの1%未満であり、この話題性のあるルアーは、ユーザを騙して悪意のあるリンクや添付ファイルをクリックさせる効果が低いことが示唆されています。マルウェア配信者は、クリック率を最大化したいというモチベーションを持っているため、様々な地域で汎用的に効果が証明されているルアーを使いたがります。

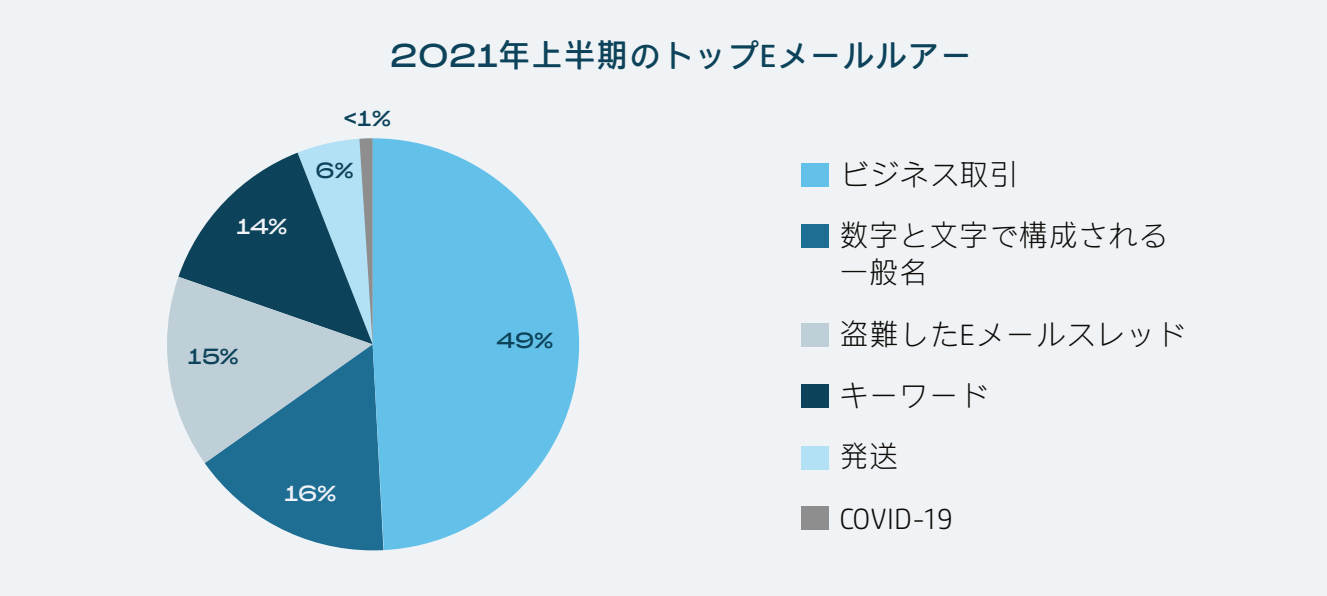


図11 – 2021年上半期にHP Wolf Securityが隔離したトップEメールルアー

法執行機関によるテイクダウンによりDridexがEmotetを追い抜く

2021年1月27日に法執行機関によって**Emotet**がテイクダウンされる以前は、Eメールスレッド・ハイジャックと呼ばれる手法で、盗まれたEメールスレッドから作成されたルアーを使用して、日本の組織をターゲットにした大規模なEmotetキャンペーンが行われていました。[8] テイクダウン後、Word文書を介して配布されるマルウェアの割合が大幅に減少しました。これは、Emotetの運営者がWordベースのダウンローダーを好んで使用していたためです。

2021年第1四半期にEmotetの活動が低下したことで、DridexがHP Wolf Securityが隔離したマルウェアファミリーのトップになりました。2012年にバンキング型トロイの木馬として誕生しましたが、2017年以降、Dridexの運用者は、優先的な収益化方法をランサムウェア攻撃に移行するケースが増えています。[9] Emotetは関連する組織的脅威グループのマルウェアを配布することが知られており、そのビジネスモデルが、かつてバンキング型トロイの木馬により侵害したホストへのアクセスを販売することであることを示唆しています。

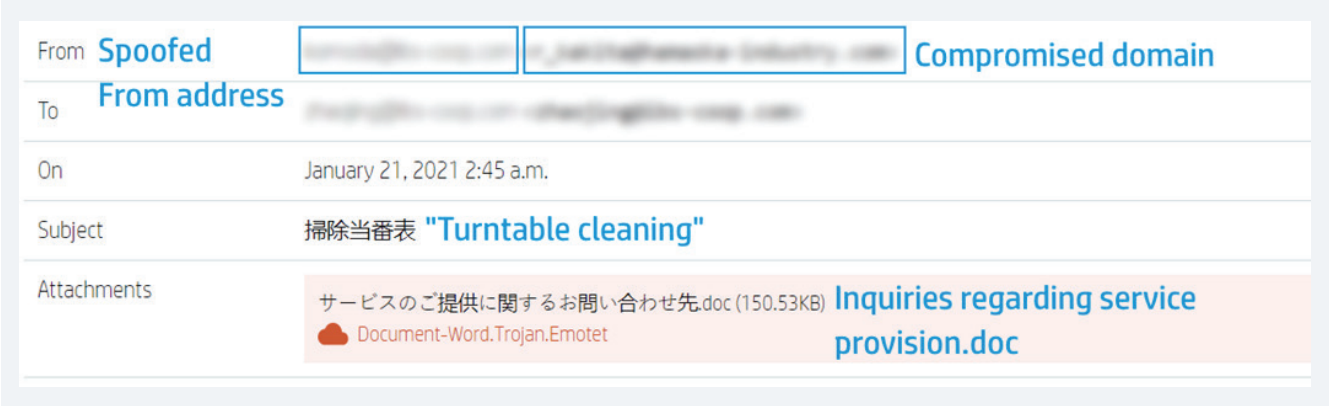
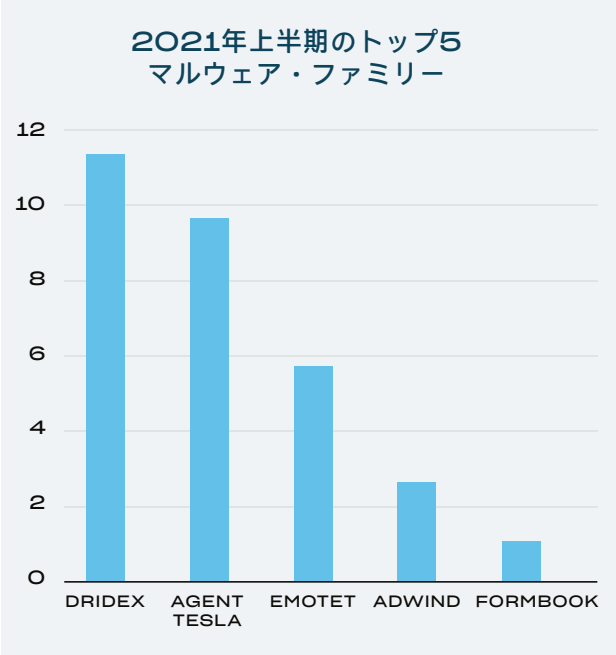


図 12 – Emotetは信憑性のある日本語のフィッシングテンプレートを作成するために盗まれたEメールのデータを利用

脅威アクターは引き続きMicrosoft Officeの古い脆弱性をエクスプロイト

脅威アクターは、Microsoft Officeの古い脆弱性をエクスプロイトし続けており、企業が環境内の古いOfficeバージョンにパッチを当てる必要性を示しています。2020年下半期と比較して、2021年上半期には、**CVE-2017-11882**のエクスプロイトが24%増加しました。それ以外では、報告期間中に攻撃者によってエクスプロイトされた脆弱性に大きな変化はありませんでした。



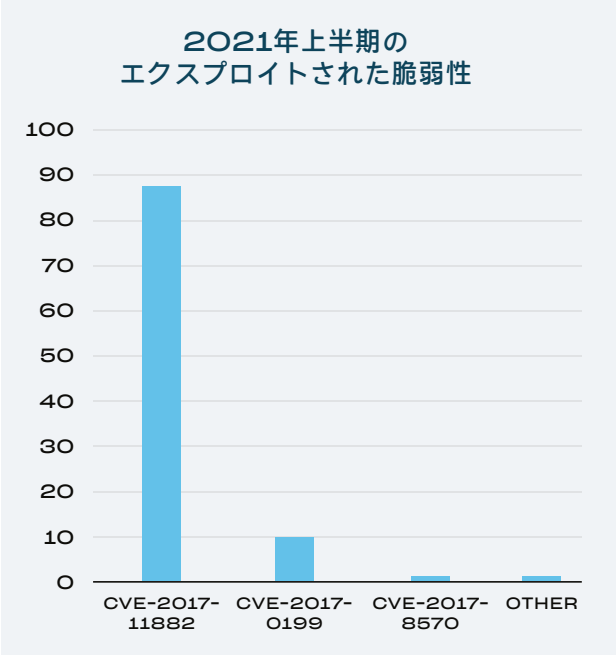


図13 & 14 – 2021年上半期にHP Wolf Securityが隔離した上位のマルウェア・ファミリーとエクスプロイトされたCVE

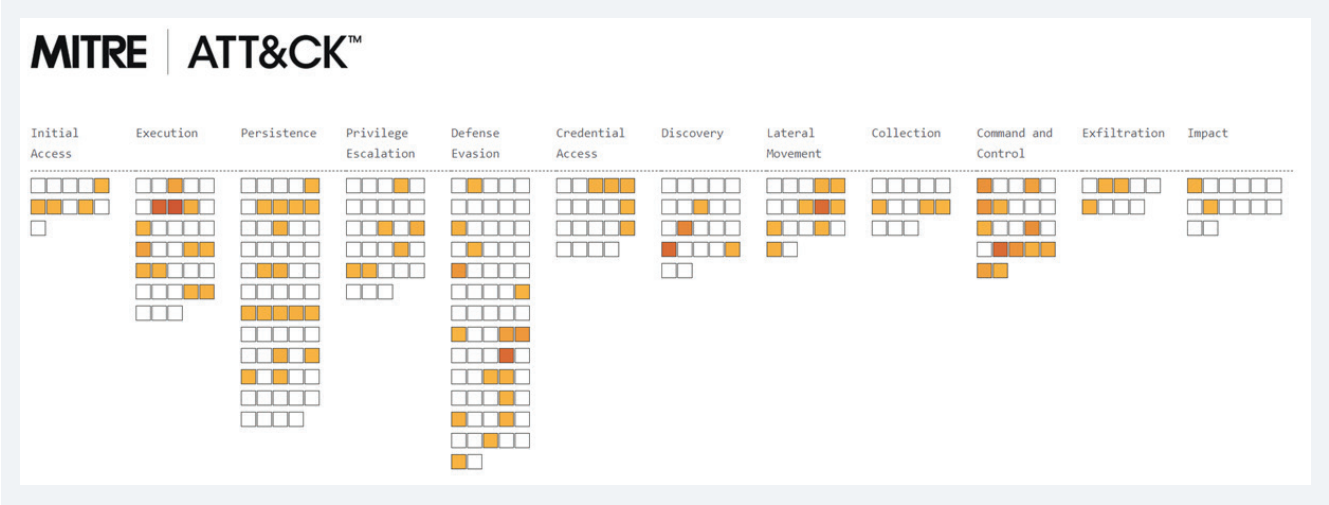


図15 – 2021年上半期にHP Wolf Securityによって隔離された脅威が使用したMITRE ATT&CKテクニック[10]

注目すべきテクニック

TA551とTA505のドメイン・インフラストラクチャの検知

脅威アクターは習慣性があり、確立された行動パターンに従う傾向があります。HP Threat Researchチームは、**TA551**と**TA505**という2つの脅威グループが使用するドメインを、マルウェアキャンペーンに使用される前に事前に検知する技術を発見しました。ドメインに含まれるキーワード・パターン、優先的に使用するDNSプロバイダー、ドメイン・レジストラを調査することで、これらのグループのドメイン・インフラストラクチャを特定することができました。

TA505は、2014年に初めて確認された金銭的な動機を持つ脅威グループです。 近年では、ランサムウェア**ClOp**を感染させて被害者から恐喝することで収益を得ています。このグループは通常、**Get2**や**SDBBot**といったマルウェアを使って被害者のネットワークにアクセスします。 このグループは、キャンペーンの前に、マルウェアのコマンド＆コントロールに使用する新しいドメインを登録していました。

TA551は、2019年に入ってから活動を開始したマルウェア配布グループです。**Ursnif**、**Valak**、**IcedID**、**Qakbot**などのマルウェアファミリーを拡散しているのが確認されています。

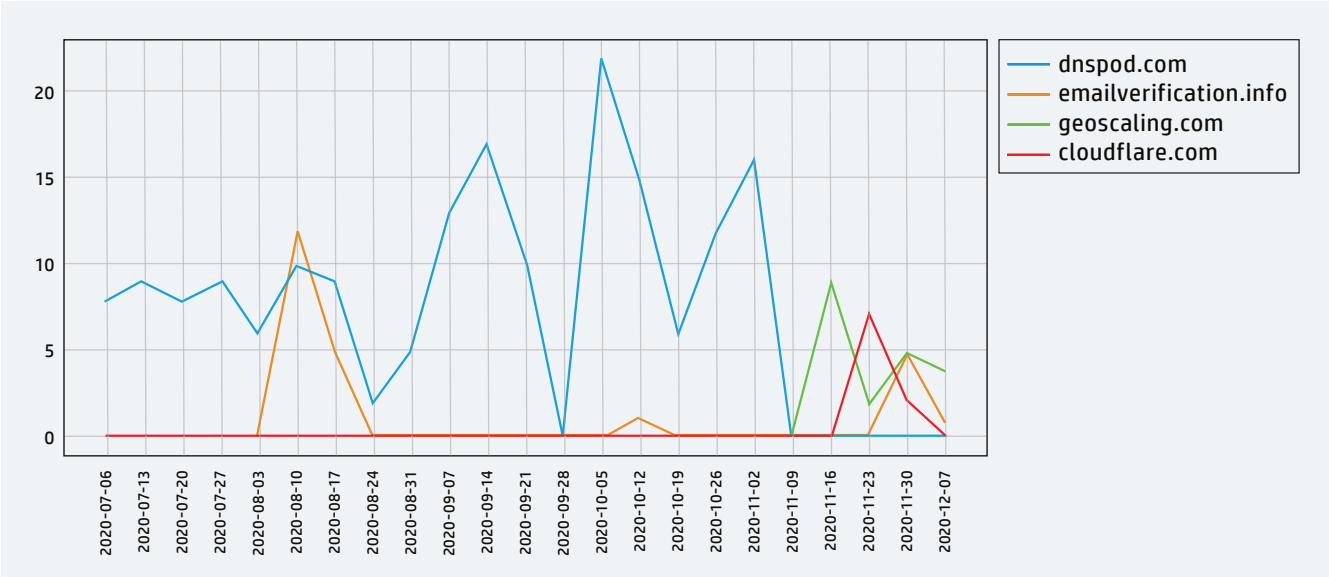


図16 – TA551の優先的なDNSプロバイダーの経時変化

インディケーターとツール

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のに役立つ侵害の痕跡（IOC）、シグネチャ、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。[11]

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、脅威をHPと共有することを選択したお客様によって実現されています。HPに転送されたアラートは、当社のセキュリティ専門家によって分析され、それぞれの脅威に関する追加のコンテキスト情報が注釈されます。

お客様には、**HP Wolf Enterprise Security**[a] の導入効果を最大限に得るために、以下のアクションを取ることをお勧めします：

- **HP Wolf Security Controller**[b]でThreat Intelligence ServicesとThreat Forwardingを有効にします。 これらの機能により、脅威のトリアージとラベリングを自動化するための脅威インテリジェンスの強化と、正確な検知と最新の攻撃手法に対する保護を保証するためのルールの自動更新が可能になります。詳細については、これらの機能に関するナレッジベースの記事をご覧ください。[12, 13]

- 新しいリリースごとにHP Wolf Security Controllerをアップデートすることで、新しいダッシュボードやレポート・テンプレートを受け取ることができます。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いただけます。[14]

- HP Wolf Securityのエンドポイント・ソフトウェアを少なくとも年に2回アップデートし、当社の脅威研究チームが追加した検知ルールに対応してください。最新の脅威研究については、**HP Wolf Security blog**で、当社のセキュリティ・エキスパートが定期的に新しい脅威を分析し、その結果を共有しています。[15]

THE HP WOLF SECURITY 脅威インサイトレポートについて

企業は、ユーザーが電子メールの添付ファイルを開いたり、電子メール内のハイパーリンクをクリックしたり、ウェブ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、リスクのあるアクティビティをマイクロVMに隔離することで、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。マルウェアを封じ込めることにより、HP Wolf Securityは豊富なフォレンジックデータを収集し、顧客のインフラストラクチャの強化を支援します。HP Wolf Security脅威インサイトレポートでは、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ており、お客様が新たな脅威を認識し、環境を保護するための対策を講じることができます。

HP WOLF SECURITYについて

HP Wolf Securityは、世界で最も安全なPC[c]とプリンタ[d]のメーカーが提供する新しいタイプのエンドポイント・セキュリティです。[e] 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、企業がPC、プリンタ、そして人を、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://owasp.org/www-community/attacks/Credential_stuffing

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

[4] https://apt.thaicert.or.th/cgi-bin/listgroups.cgi?t=DanaBot&n=1

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

[6] https://threatresearch.ext.hp.com/purple-fox-exploit-kit-now-exploits-cve-2021-26411/

[7] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26411

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

[9] https://us-cert.cisa.gov/ncas/alerts/aa19-339a

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

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

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

[13] https://enterprisesecurity.hp.com/s/article/Bromium-Threat-Intelligence-Cloud-Service

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

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

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。HP Sure 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. Windowsおよび第8世代以上のインテル® プロセッサーまたはAMD Ryzen™ 4000プロセッサー以上を搭載したHP Elite PC、インテル® 第10世代以上のプロセッサーを搭載したHP ProDesk 600 G6、およびAMD Ryzen™ 4000またはインテル® 第11世代以上のプロセッサーを搭載したHP ProBook 600に搭載された、追加コスト・追加インストールなしの標準装備されたHP独自の包括的なセキュリティ機能に基づいています。

d. HP の最先端の組み込みセキュリティ機能は、HP FutureSmart fi rmware 4.5 以上を搭載した HP Enterprise および HP Managed デバイスで利用可能です。2021年に公開した競合する同クラスのプリンター機能の米国HP Inc.によるレビューに基づきます。HPのみが、デバイスのサイバーレジリエンに関するNIST SP 800-193ガイドラインに従って、攻撃を自動的に検知し、停止し、自己回復型リブートするセキュリティ機能を提供しています。対応製品のリストについては、hp.com/go/PrintersThatProtectをご覧ください。詳細については、hp.com/go/PrinterSecurityClaimsをご覧ください。

e. 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 WOLF SECURITY

© Copyright 2021 HP Development Company, L.P.