HP WOLF SECURITY

脅威インサイトレポート

Q4 - 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3Q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年第3四半期に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]

特筆すべき脅威

Excelアドイン（.XLL）を利用しシステムを感染させる攻撃者が急増中

2021年第4四半期、HP Wolf Securityは、悪意のあるMicrosoft Excelアドイン（XLL）ファイルを使用してシステムに感染するマルウェアキャンペーンを第3四半期と比較して6倍近く（588%）増加させたことを検知しました。この手法は、MITRE ATT&CKではT1137.006[2]として分類されています。
アドインの意図は、アプリケーション・プログラミング・インタフェース（API）を介してExcelワークシートから呼び出される高性能な関数を包含することです。このアドインはマルチスレッドなどの機能をサポートするため、VBA（Visual Basic for Applications）のような他のスクリプト・インターフェースより優れたExcel機能の拡張を、ユーザーに提供します。攻撃者が正規のAPIやスクリプト機能を利用することは目新しいことではありませんが、この手法が人気を集めているということは、脅威アクターがソフトウェアの正規の機能を悪用して目的を達成する方法を常に探していることを物語っています。

588%

2021年第4四半期にHP WOLF SECURITYが検知したXLLマルウェアは第3四半期と比較して上昇。

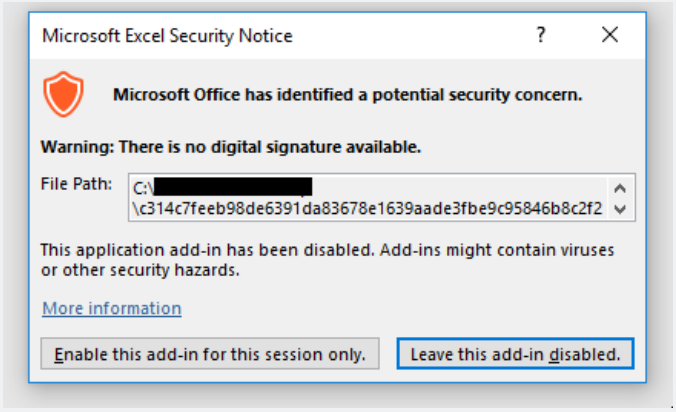
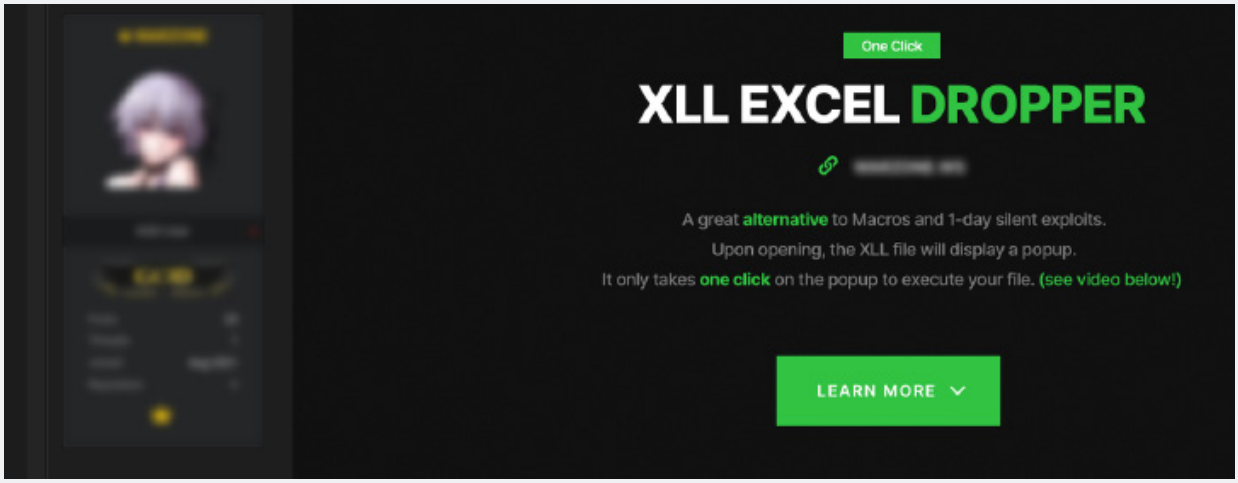


図1 – ユーザーがXLLファイルを開く際に表示される画面

我々が分析したキャンペーンでは、悪意のあるXLLの添付ファイルまたはリンクが添付されたメールがユーザに送信されていました。[3] 添付ファイルをダブルクリックすると、Microsoft Excelが開き、ユーザにアドインのインストールとアクティベーションを促します。 攻撃者は通常、アドインが起動すると直ちに実行される xlAutoOpen 関数内にコードを配置します。この手法が危険なのは、ユーザーがMicrosoft Officeの「保護ビュー」を無効にしてマクロコンテンツを有効にする必要があるVBAマクロとは異なり、マルウェアの実行に必要なのは1回のクリックだけであることです。しかしながら、一部のメールゲートウェイでは、XLLファイルはダイナミックリンクライブラリ（DLL）であり、メールで送信されることはほとんどないファイルタイプであるため、すでにブロックされています。以下の緩和策を検討することを推奨します。

- XLLの添付ファイルを含むメールの受信をブロックするようにメールゲートウェイを設定をする。
- 信頼できる発行者の署名入りのアドインのみを許可するようにMicrosoft Excelを設定する。
- 独自のアドインを完全に無効にするようにMicrosoft Excelを設定する。

2021年第4四半期には7種類（**Dridex**、**IcedID**、**BazaLoader**、**Agent Tesla**、**Raccoon Stealer**、**Formbook**、**Bitrat**）のシステムへの初期感染時に悪意のあるExcelアドインを介して配信れるマルウェアファミリーを確認しました。また、アンダーグラウンドのフォーラムでは、XLLマルウェアやサービスを宣伝する広告が掲載されており、中には**$2,100 USD**ほどで提供されるビルダーもありました。図2はあるマルウェア作者による、システムにマルウェアを配信するためのXLLドロッパーと称する、フォーラムへの投稿です。ユーザーは、配信したいマルウェアのペイロードへの実行ファイルまたはリンクと、アドインを開いた後にユーザーを騙すためのおとり文書を指定します。このツールは、攻撃に使用可能な悪意のあるXLLファイルを生成します。第4四半期にExcelアドイン・マルウェアが増加していることから、脅威アクターはこの手法を模索していると考えられます。しかし、Excel4のマクロやDynamic Data Exchange（DDE）、VBAなど十分に使いこなされた配信手法を上回ることができるかどうかは未知数です。それでも、企業はこのような攻撃に常に注意を払う必要があります。



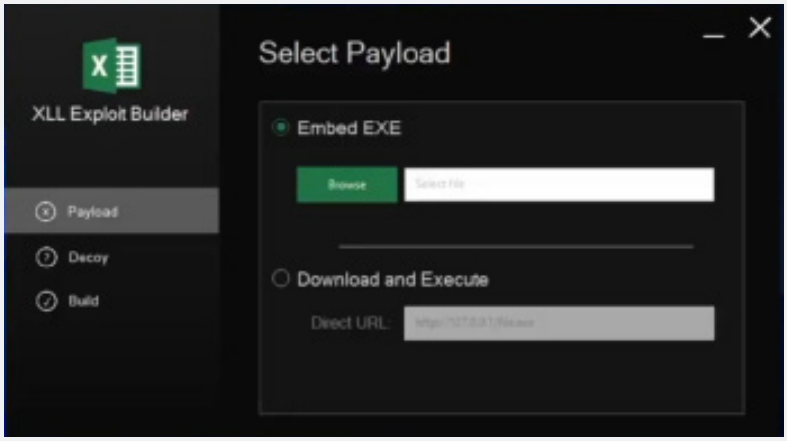


図2&3 – XLLドロッパーを宣伝するフォーラムの投稿（上）と、そのユーザーインターフェースのスクリーンショット（下）

QakBotは攻撃者に感染したシステムへのアクセスを提供しランサムウェアを配信する

QakBotは、2021年第4四半期にHP Wolf Securityが隔離した上位のマルウェアファミリーの1つです。2021年1月にグローバルな法執行活動によって**Emotet**ボットネットのインフラストラクチャが破壊された後、QakBotはマルウェア運営者が感染したシステムにアクセスするための代替手段として登場しました。Emotetと同様に、QakbotはEメールのスレッドをハイジャックすることができます。このマルウェアは、盗んだメールの会話を使って偽の返信を生成し、ルアーの信頼性と感染の可能性を高めます。第4四半期に配信された悪質なスパムメールには、**Microsoft Excel Binary Workbook (XLSB)**ファイルを含むZIPアーカイブをダウンロードするリンクが含まれていました。このワークブックが解凍されて開かれると、悪意のあるマクロがトロイの木馬QakBotを含むDLLをダウンロードし、名前を変えて実行します。QakBotは、システム上に隠れるために、**プロセスインジェクション**と呼ばれる技術を用いて、正規のプロセス（分析したサンプルではexplorer.exe）にコードを書き込みます。（図4）この正規のプロセスを装いPCに永続的に残るために、マルウェアはスケジュールされたタスクを作成します。

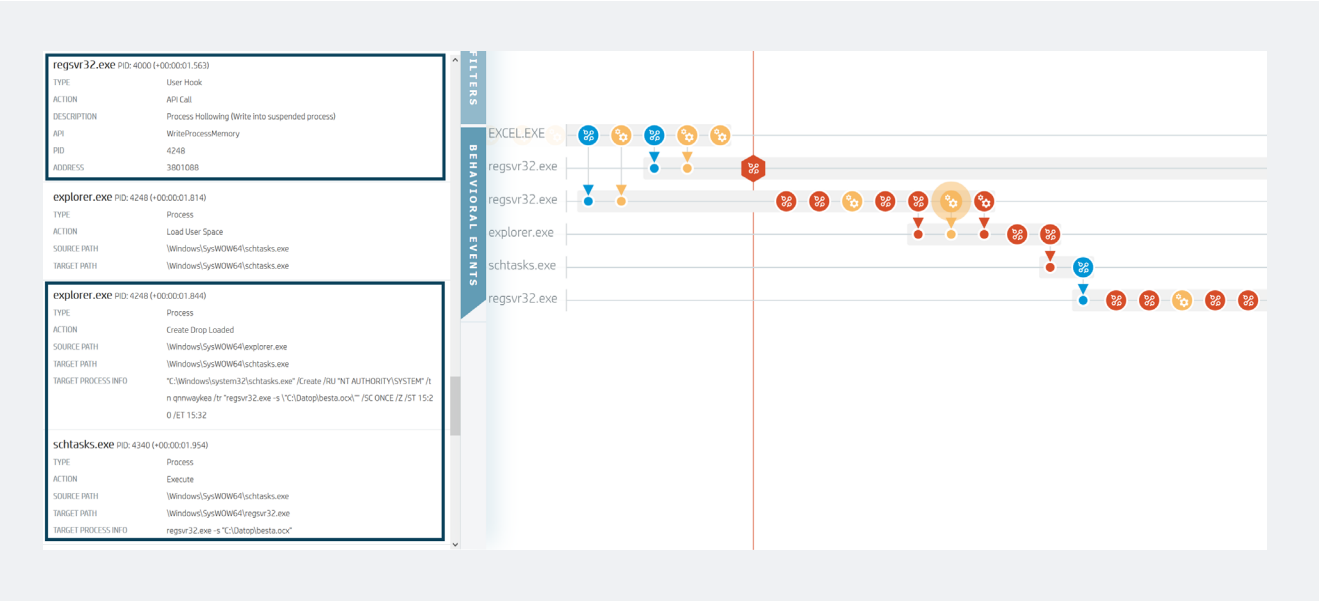


図4 – 隔離されたHP Sure ClickマイクロVM内で動作する2021年第4四半期のQakBotサンプル

QakBotの運営者は、このマルウェアに感染したコンピュータへのアクセス権を他の脅威アクターに販売することで、ボットネットを収益化していると考えられます。これは、システムへのアクセスを必要とする他の脅威アクターにサービスを販売するという、**サイバー犯罪者の専門化**の幅広い傾向の一例です。QakBotの感染チェーンは、ランサムウェア **Conti** につながることが確認されており、彼らの顧客にランサムウェアのアフィリエイトが含まれていることが示唆されています。2021年11月にEmotetが復活したにもかかわらず、QakBotはセキュリティチームが注意して見守るべき脅威であり続けています。

Aggahが悪意のあるPowerPointアドイン（.PPA）で韓国の組織を狙う

Aggahは、パキスタンを拠点とすると理解されている脅威グループ Green Havildar に関連する金銭的動機を持った脅威アクターです。[4] 我々は以前、2020年7月にAggahがヨーロッパの組織を標的に戦術、技術、手順（TTP）を変更したことを記事にしました。[5] 2021年12月にHP Wolf Securityが検知したキャンペーンでは、Aggahは韓国語を話す組織を対象に偽の発注書を作成していました。発注書は、リモートアクセス型トロイ木馬（RAT）である**Agent Tesla**の配信に使用される悪意のあるPowerPointアドインファイル（.PPA）でした。このファイルを開くと、Windowsに組み込まれたMicrosoft HTML Applicationエンジンであるmshta.exeを使って、悪意のあるVBAマクロがVBScriptの実行を引き起こします。興味深いことに、攻撃者は悪意のあるコードを独自のインフラストラクチャに保存するのではなく、HTMLページに埋め込まれた悪意のあるVBScriptやPowerShellスクリプトを、blogspot[.]comサブドメイン経由でブログホスティングサイトBloggerに保存していました。PowerPointのマルウェアは珍しく、2021年第4四半期にHP Sure Clickで隔離されたマルウェアの1%です。

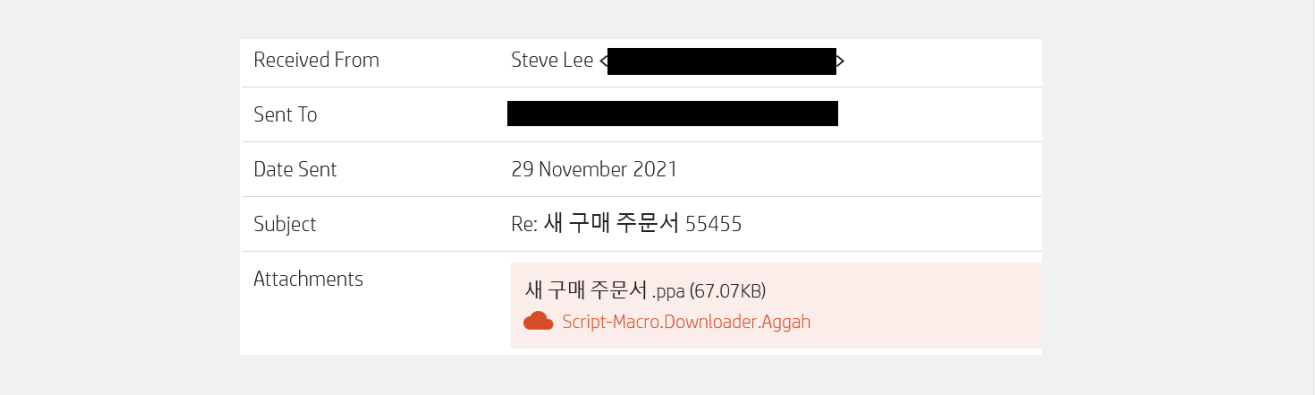


図5 – Aggahが悪意のあるPowerPointアドインによりAgent Teslaマルウェアを配信するために使用した韓国語ルアー

TA505のMirrorBlastとのつながり

2021年9月中旬から11月中旬にかけて、 **MirrorBlast** と呼ばれる全く新しいマルウェア・キャンペーンが発生し、その特異なツールや手法からセキュリティ研究者の注目を集めました。いくつか違いはあるものの、この新しいキャンペーンのTTPは、経済的動機を持つ脅威アクターとして知られる**TA505**が仕組んだ古いキャンペーンと多くの類似点がありました。これらの類似点には、攻撃者がインフラを構築するために行った手順、ドメイン登録のパターン、キャンペーンの頻度、ダウンロードサイトやルアードキュメントの類似性、ターゲット選択メカニズム、フォローアップ・マルウェアの類似性などが含まれます。これらの類似点を総合すると、TA505がMirrorBlastの背後にいることが一定の確信を持って示唆されます。これが事実であれば、MirrorBlastキャンペーンは、感染率を高く保つために新しいツールや技術への投資を惜しまない脅威アクターの姿を示しています。2021年11月以降、MirrorBlastの活動が確認されていないため、これがテストキャンペーンだったのか、TA505による実験だったのかという疑問が生じています。私たちの調査の詳細は、HP Wolf Security Blogでご覧いただけます。[6]

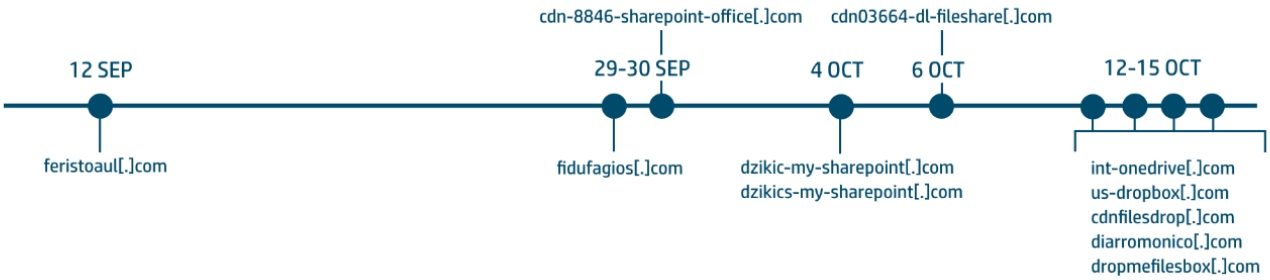


図6 – 2021年9月 ~ 10月のMirrorBlastドメインの登録を示すタイムライン

イタリア語圏の組織にUrsnifマルウェアを送り込む進行中の宅配便スパム

第4四半期、HP Wolf Securityは、バンキング型トロイの木馬 **Usrnif** を配信する**Cutwail**ボットネットから発信された、イタリアの組織を標的とした大規模な継続的スパムキャンペーンを検知しました。このキャンペーンは、主に製造業や地方自治体など少なくとも248組織のイタリア語を話すユーザーを対象としていました。攻撃者は、イタリアの宅配会社であるBRTの送信者ドメインを偽装し、ユーザーを騙してEメールを開かせました。各Eメールには、正規表現 **XSG\d{7}\.xls** に従って命名されたExcel（.XLS）スプレッドシートの添付ファイルが含まれていました。この添付ファイルをMicrosoft Excelで開くと、悪意のあるマクロがダウンロードされ、システム上でUrsnifのペイロードが実行されます。件名は正規表現に従い、**BRT - Abbiamo preso in carico la tua spedizione (ID\d{7})**、英語では "We have taken charge of your shipment" と訳されます。Ursnifは、銀行の Webサイトのログイン認証情報を盗むことができるバンキング型トロイの木馬です。

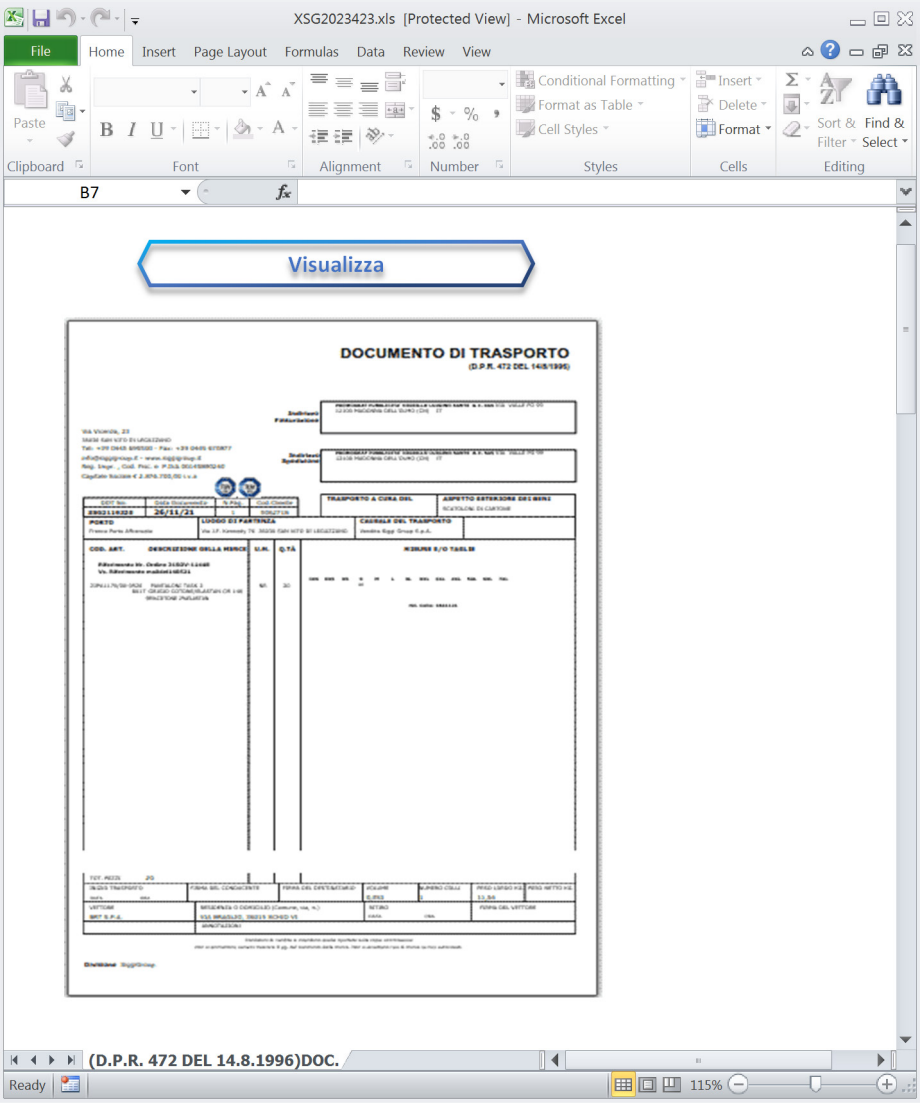


図7 – Ursnif マルウェアをダウンロードする偽の宅配便ルアー

Emotetリターンとその役割の逆転

2021年11月15日、HP Sure Clickは、約10か月ぶりに大企業を標的とした新たな **Emotet** キャンペーンを隔離しました。[7] 変更点の1つは、Emotet の運用者がマルウェアの配信に、従来使用していたWordやJavaScriptのダウンローダーではなく、Excelのダウンローダーを使用するようになったことです。また、TTPの変化としては、**TrickBot**に感染したPCの一部がEmotet を展開するようになったことが挙げられます。これは、2020年1月以前に見られたものとは逆の現象です。当時は、「3つの脅威」と呼ばれた感染チェーン、つまりEmotet が最初の侵害を行い、TrickBotを投下し、続いてランサムウェアを投下していました。また、セキュリティ研究者によると、Emotetのサンプルは、TrickBotのような中間段階のマルウェアではなく、バックドアであるCobalt Strike Beaconをドロップすることも確認されています。[8] この変更は、被害者ネットワークへの滞留時間を最小限に抑え、Emotet の顧客がランサムウェアを展開するのにかかる時間を短縮するため攻撃者にとってメリットがあります。また、中間的なマルウェアを展開しないことで、セキュリティツールに検知される可能性も低くなります。

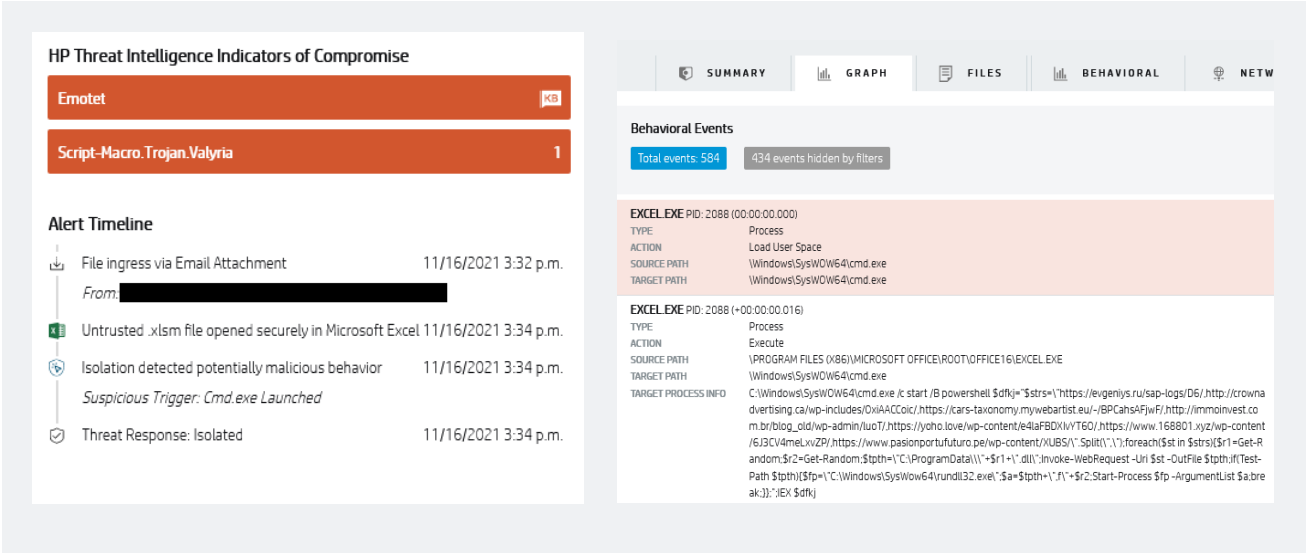


図8 & 9 – 2021年11月にHP Sure Clickで隔離したEmotetサンプル

偽のDiscordサイトがインストーラーを装ったRedLineマルウェアを提供

2021年12月、人気のメッセージングアプリケーション Discord のインストーラーを装って情報を盗む **RedLine** を拡散するマルウェアキャンペーンを発見しました。この偽装Webページは、Discordの正規のWebサイトを模倣しており、無防備な訪問者を騙して「ダウンロード」ボタンをクリックさせ、悪意のあるインストーラーを配信するように設計されていました。攻撃者は、12月1日に偽のインストーラー DiscordSetup.js をzipファイルで提供する、**discrodappp[.]com** というタイポスクワッティングされたドメインを登録しました。このJScriptファイルをクリックすると、バッチスクリプトを実行する実行ファイルがダウンロードされます。このバッチスクリプトは、AutoITの実行ファイルを生成し、エンコードされ圧縮されたRedLineペイロードを含むAutoITスクリプトを実行します。このマルウェアは、Windows API関数のRtlDecompressBufferを使用して解凍されます。

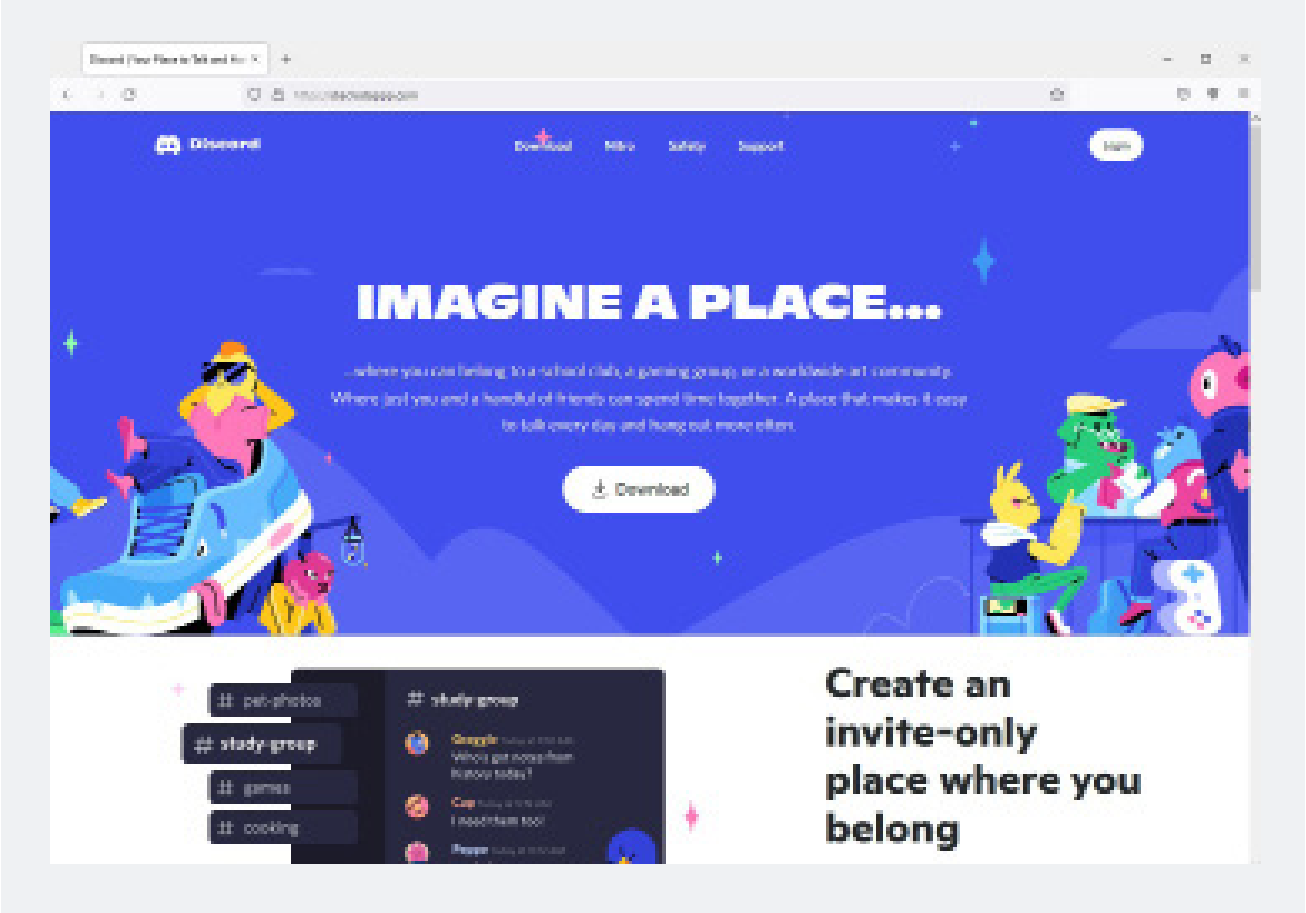


図10 – 偽のDiscord WebサイトがRedLineマルウェアを無防備な訪問者に提供

注目すべきトレンド

第4四半期にHP Wolf Securityが検知したCVE-2017-11882 Equation Editor Exploitsは第3四半期に比べて4%増加し、CVE-2017-0199 Rich Text File Exploitsは14%増加しました。また、今期は悪意のあるOfficeドキュメントが増加しており、Microsoft Wordを標的とした脅威は第3四半期と比較して6%増加し、Excelを標的とした脅威は4%増加しています。アーカイブは、マルウェアの経路としてはあまり人気がなく、第4四半期には10%減少しました。

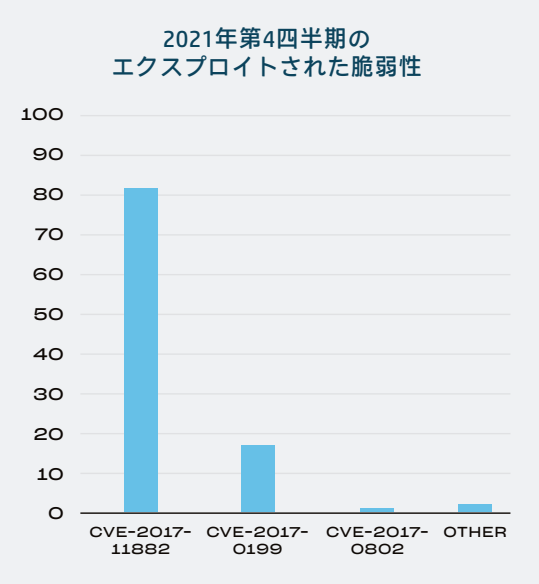
第4四半期には、ゲートウェイのセキュリティ管理策をバイパスするEメールの脅威がわずかに増加しました。2021年第4四半期にHP Sure Clickによって隔離されたEメールベースのマルウェアのうち、少なくとも1つのゲートウェイスキャナを回避したものは、第3四半期の12%に比べて13%でした。さらに、HP Sure ClickがブロックしたEメールマルウェアのうち2%は、Sender Policy Frameworkのチェックに失敗したにもかかわらず、ユーザーの受信トレイに配信されていました。

Eメールは依然として感染経路のトップであり、第4四半期にHP Sure Clickによって隔離された脅威の77%がこの経路を利用していました。脅威の13%はWebブラウザ経由でダウンロードされ、11%は悪意があるとわかっているファイルを開いてしまうなど、ユーザーが原因となっていました。

Eメールルアーのキーワード TOP 10

1. “ORDER”
2. “2021”
3. “PAYMENT”
4. “NEW”
5. “2021/2022”
6. “REQUEST”
7. “INVOICE”
8. “QUOTATION”
9. “PURCHASE”
10. “DEC”

図 11 – 第4四半期にHP Wolf Securityによって隔離された脅威の中のトップEメール件名ルアー



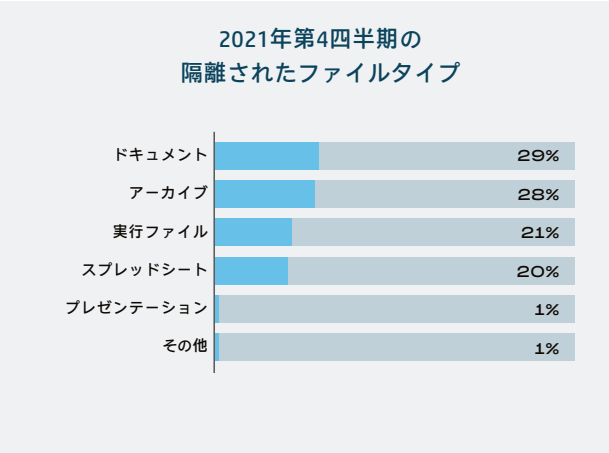


図12 & 13 – 2021年第4四半期にHP Wolf Securityが隔離した上位のエクスプロイト（左）とファイルタイプ（上）

2021 脅威の傾向とアウトルック

過去12ヶ月間のHP Wolf Securityと外部の脅威データを振り返って、組織が注意すべき主要なセキュリティ・トレンドを紹介します。

サプライチェーンを狙った攻撃はより一般的になり被害者はより大きな侵害を受けた

歴史的に、サプライチェーン攻撃は持続的標的型攻撃（Advanced Persistent Threat）に関連していましたが、7月にKaseyaで発生したREvilランサムウェアのように、2021年に注目を集めた攻撃は、資金力のある有能な犯罪者がサプライチェーンをいかに悪用できるかということを明らかにしました。マネージドサービスプロバイダー（MSP）は、悪意のあるアクターにとって魅力的な伝播経路であり続けています。情報の窃盗に重点が置かれていたこれまでのサプライチェーンを狙った攻撃に比べ、 最近のサプライチェーン攻撃の例は、攻撃を収益化する方法としてランサムウェアが普及していることから、直接的な影響が大きくなっています。[9][10] 2021年には、UA-Parser-JSというJavaScriptパッケージのように、人気のあるソフトウェアパッケージが悪意のあるコードでハイジャックされた例も見られ、企業がソフトウェアに依存する中で、トロイの木馬に感染したコードの検知に直面しているということが浮き彫りになりました。[11] 企業がサプライチェーンの危険性を低減する方法の一つは、サービスを購入する前に、MSPとベンダーを徹底的に評価するということです。利用しているソフトウェアを最新に維持することで、トロイの木馬化に感染したソフトウェアの検知と修復を迅速に行うことができます。

2021に HP WOLF SECURITYが検知したランサムウェアの配信に使用されたマルウェアファミリー

DRIDEX
QAKBOT
EMOTET
ICEDID
TRICKBOT
BAZALOADER

強化されたランサムウェア運営者とアフィリエイトが重要インフラを破壊し、政府や法執行機関の強力な対応につながる

ランサムウェアは、ネットワークへのアクセスをサイバー犯罪者が収益化するためのツールであることに変わりはありません。ランサムウェアはシステムを無力化するものであるため、非常に大量の攻撃が行われている現状では、一部の侵入行為が重要サービスに影響を与える結果となり得ます。医療分野では、2021年5月にアイルランドのHealth Service Executive（公営医療サービス）に対するランサムウェア攻撃により、病院の予約がキャンセルされ、520人の患者の記録が流出し、被害額は €1億EURと推定されています。[12] 2021年に最も注目を集めたランサムウェアによるインシデントは、2021年5月にコロニアル・パイプラインに影響を与え、パニック買いによって燃料不足を引き起こしました。犯人のDarkSideというグループによって100GBのデータが盗まれ、$440万 USDの身代金が支払われました。[13] この攻撃をきっかけに、バイデン米大統領は米連邦政府とそのサプライヤーの防御力を向上させるための大統領令第14028号を発令しました。[14] これらの介入の結果として考えられるのは、ランサムウェア運営者が、法執行機関や政府の怒りを買いそうなターゲットからシフトするということです。

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。[15]

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。[16][17]

• 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。[18]

• 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。[19]

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://attack.mitre.org/techniques/T1137/006/

[3] https://threatresearch.ext.hp.com/how-attackers-use-xll-malware-to-infect-systems/

[4] https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf

[5] https://threatresearch.ext.hp.com/aggah-campaigns-latest-tactics-victimology-powerpoint-dropper-and-cryptocurrency-stealer/

[6] https://threatresearch.ext.hp.com/mirrorblast-and-ta505-examining-similarities-in-tactics-techniques-and-procedures/

[7] https://threatresearch.ext.hp.com/emotets-return-whats-different/

[8] https://www.bleepingcomputer.com/news/security/emotet-now-drops-cobalt-strike-fast-forwards-ransomware-attacks/

[9] https://www.pwc.co.uk/issues/cyber-security-services/insights/operation-cloud-hopper.html

[10] https://www.reuters.com/article/uk-usa-cyber-treasury-exclusive-idUKKBN28N0PI

[11] https://www.cisa.gov/uscert/ncas/current-activity/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js

[12] https://www.irishtimes.com/news/crime-and-law/hse-confirms-data-of-520-patients-published-online-1.4578136

[13] https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown

[14] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

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

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

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

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

[19] 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。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 SecurityController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スに関する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