

脅威インサイト レポート

2020年10月





脅威のランドスケープ

HP-Bromium Threat Insights Reportの2020年10月版へようこそ。このレポートでは、2020年の第3四半期（7月1日～9月30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。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

Emotetスパムキャンペーンは日本とオーストラリアの組織に集中

2020年の第3四半期には、特に8月末に、Emotetマルウェアを配布する悪質なスパムキャンペーンが大幅かつ持続的に増加しました（図1）。HP Sure Clickによって隔離されたEmotetのサンプル数は、第3四半期には第2四半期と比較して1,200%以上増加しました。Emotetスパムの活動は、2020年3月以降断続的に行われていました。2018年以降のEmotetスパムのパターンから、2021年初頭まで毎週のようにスパムが実行される可能性が高いことが示唆されています。

バンキング型トロイの木馬としての起源にもかかわらず、2017年以降、Emotetは他の脅威グループに感染したシステムへのアクセスを提供するためのローダーとして使用されることが多くなっています。¹ これまでのところ、2020年にはEmotetを介して展開された二次的なTrickBotとQakBot感染が確認されています。² 注目すべきは、Emotetの感染は、人間が操作するランサムウェア攻撃の前兆であることが多いことです。³ 脅威アクターは、Ryuk⁴などのランサムウェアファミリーを展開する前に、感染したシステムへのアクセスを利用して被害者のネットワークを偵察していることが確認されています。

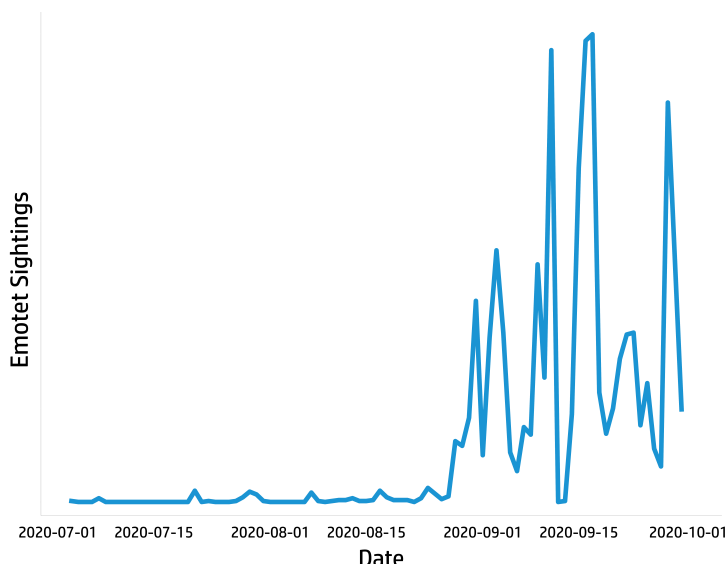


図1 - 2020年Q3にHP Sure Clickで隔離されたEmotetサンプル

% Q3 2020 Emotet Recipients by Top-level Domain

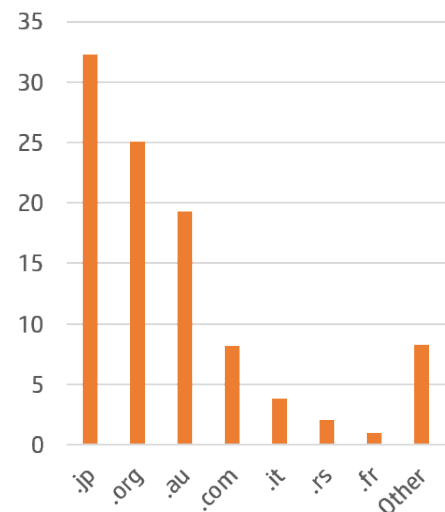


図2 - HP Sure Clickテレメトリーによるトップレベル・ドメイン別 2020年Q3Emotetスパム受信者

日本とオーストラリアの組織は、2020年第3四半期に復活したEmotetスパム活動の影響を最も受けています。HP Sure Clickテレメトリーの分析によると、サンプルの32%が.jpコードトップレベルドメイン(ccTLD)を使用したドメインに送られており、受信者の20%近くが.au ccTLDを使用していたことがわかりました（図2）。個人アドレスではなく組織がターゲットとされており、Emotetスパムの4分の1は.orgドメインに送られていました。組織をターゲットにしているのは、ランサムウェアの実行者が貴重なデータを保有している可能性が高いため、侵害されたシステムへのアクセスを仲介するという、Emotetの運営者の目的と一致しています。

Emotetは、電子メールに添付またはリンクされた悪意のあるWord文書を実行させることで、

注目すべきテクニック

Word文書を暗号化して検知を回避

脅威アクターは、システムへの侵入を成功させる可能性を高めるための方法を継続的に実験しています。2020年9月のTrickBotキャンペーンは、その規模にもかかわらず、Word文書のドロPPERが検知を回避するのに効果的でした。サンプルの70%は4つ以下のスキャンエンジンによってしか悪意のあるものと識別されず、いくつかのファイルでは検知がゼロになっていました（図9）。

検知率が低いのは、主にMicrosoft Wordの「パスワードで暗号化」機能を使って文書が暗号化されていたためです。この場合、文書の内容と拡張メタデータは、CBCモードのAESを使用して256ビットのキーで暗号化されていました。悪意のあるファイルを添付した電子メールにはパスワードが書かれており、受信者が復号化して開くことができるようになっていました。このキャンペーンで発見された最も一般的なパスワードは、正規表現[A-Z]{3}|d{2}と一致する5文字の長さのものでした（例：「DLW16」）。

パスワードがないと、静的エンジンとふるまいエンジンはファイルの内容を検査することができません。また、この手法は、文書のパスワードがわからない場合の遡及調査を遅らせます。HP Sure Clickは、ファイルが開かれたときのアクティビティのふるまいトレースをキャプチャするため、調査者は迅速にIOCを取得し、暗号化されたファイルを含むマルウェアの能力と意図を理解することができます（図8）。

% Isolated Exploits by CVE

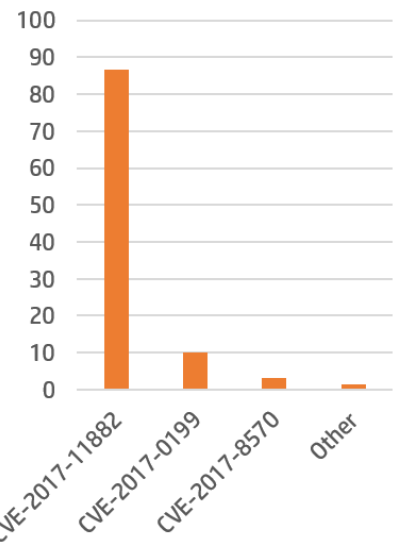


図7 - HP Sure Clickにより2020年Q3に隔離されたトップエクスプロイト

Time from triggering event	Process	Details
00:00:00.000	3340 WINWORD.EXE	ACTION: PROC_LOADIMAGE SOURCE PATH: \Windows\explorer.exe TARGET PATH: \Windows\explorer.exe
00:00:00.000	3340 WINWORD.EXE	ACTION: PROC_CREATE_DROPPED SOURCE PATH: \PROGRAM FILES\MICROSOFT OFFICE\ROOT\OFFICE16\WINWORD.EXE TARGET PATH: \Windows\explorer.exe DESCRIPTION: Dropped and Executed explorer c:\programdata\objStreamUTF8NoBOM.Vbe
+00:00:00.672	4640 explorer.exe	ACTION: PROC_LOADIMAGE SOURCE PATH: \Windows\System32\wscript.exe TARGET PATH: \Windows\System32\wscript.exe
+00:00:00.687	4640 explorer.exe	ACTION: PROC_CREATE SOURCE PATH: \Windows\explorer.exe TARGET PATH: \Windows\System32\wscript.exe DESCRIPTION: Invoked "C:\Windows\System32\WScript.exe" "C:\programdata\objStreamUTF8NoBOM.Vbe"
+00:00:40.984	4792 regsvr32.exe	ACTION: PROC_LOADIMAGE FILE SIZE: 311296 SHA-256: 7fee0f3adb6bb5a3ed22ad960709a87893e2512d099f6c8c39946097d9a4122b SOURCE PATH: \UTF8NoBOM\APSLVDFB.dll TARGET PATH: \UTF8NoBOM\APSLVDFB.dll
+00:00:41.844	4800 regsvr32.exe	ACTION: PROC_LOADIMAGE FILE SIZE: 311296 SHA-256: 7fee0f3adb6bb5a3ed22ad960709a87893e2512d099f6c8c39946097d9a4122b SOURCE PATH: \UTF8NoBOM\APSLVDFB.dll TARGET PATH: \UTF8NoBOM\APSLVDFB.dll

図8 - HP Sure Click Enterpriseの動作トレースでは、ユーザーがドロPPER文書を開いた後にregsvr32.exeにより実行されたTrickBotペイロードが隔離され示されています。



一般的なセキュリティリコメンデーション

ネットワーク防御者は、マルウェアを含む暗号化された添付ファイルによる侵害リスクを軽減するために、メールコンテンツフィルタリングポリシーの導入を検討すべきです。2020年6月、オーストラリアのサイバーセキュリティセンターは、悪意のある電子メールを軽減するための最新のガイダンスを発表しました。¹³ これらの推奨事項には、DMARCの導入、組織が受信すると予想されるファイルタイプに基づいた添付ファイルのセーフリスト化、暗号化された添付ファイルのブロックが含まれています。

シグネチャ

2020年9月キャンペーンのTrickBotドロPPER文書には、YARAルールを使用して静的に検出することが可能な特徴的なファイルアーティファクトが含まれていました。具体的には、攻撃者はハッシュベースの検知を回避するための方法として、各文書の2バイトを修正していました。そのルールを以下に公開しました。

```
rule trickbot_maldoc_embedded_dll_september_2020 {
  meta:
    author = "HP-Bromium Threat Research"
    date = "2020-10-03"
    sharing = "TLP:WHITE"

  strings:
    $magic = { D0 CF 11 E0 A1 B1 1A E1 }
    $s1 = "EncryptedPackage" wide
    $s2 = "{FF9A3F03-56EF-4613-BDD5-5A41C1D07246}" wide
    $s3 = { FF FF FF FF FF FF FF FF FF FF ( 90 90 | 10 10 | E2 E2 | 17 17 ) FF FF FF FF FF FF FF FF FF FF }

  condition:
    $magic at 0 and
    all of ($s*) and
} (filesize > 500KB and filesize < 1000KB)
```

% Malware by File Extension

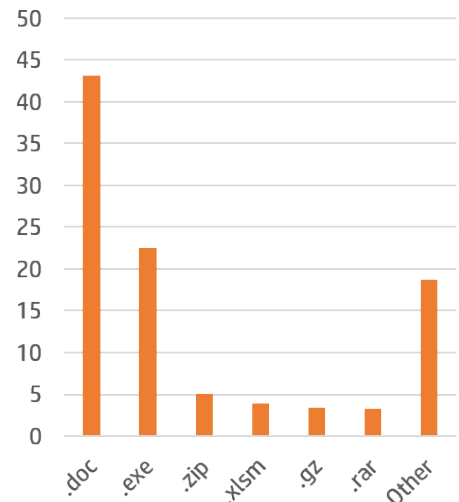


図 11 - 2020年 Q3にHP Sure Click Enterpriseで隔離されたマルウェアファイルの拡張子

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。¹⁴ 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。

- hreat 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、Customer Portal^{15 16}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。¹⁷

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。HP Sure 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://www.bromium.com/wp-content/uploads/2019/07/Bromium-Emotet-Technical-Analysis-Report.pdf>
- [2] <https://www.bleepingcomputer.com/news/security/emotet-botnet-is-now-heavily-spreading-qakbot-malware/>
- [3] <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>
- [4] <https://www.ncsc.gov.uk/files/RYUK%20Advisory%20draft%20CP%20June%202019.pdf>
- [5] <https://www.kryptoslogic.com/blog/2019/04/emotet-scales-use-of-stolen-email-content-for-context-aware-phishing/>
- [6] <https://threatresearch.ext.hp.com/detecting-a-stealthy-trickbot-campaign/>
- [7] https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html
- [8] <https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/>
- [9] <https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/>
- [10] <https://www.bbc.co.uk/news/technology-48770128>
- [11] <https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report>
- [12] <https://attack.mitre.org/>
- [13] <https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Malicious%20Email%20Mitigation%20Strategies%20%28June%202020%29.pdf>
- [14] <https://support.bromium.com/s/article/What-information-is-sent-to-Bromium-from-my-organization>
- [15] https://support.bromium.com/s/topic/0TOU0000000Hz180AC/latest-news?language=en_US&tabset=3dbaf=2
- [16] <https://enterprisesecurity.hp.com/s/downloads>
- [17] <https://threatresearch.ext.hp.com>

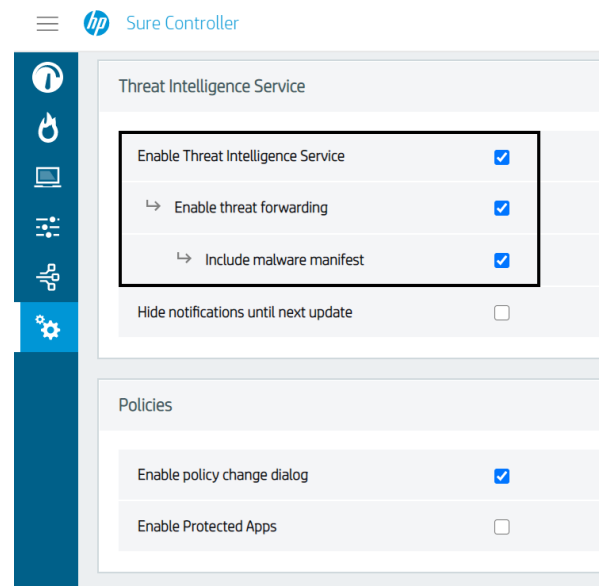


図 12 - HP Sure Controllerの推奨脅威フォワード設定