BROMIUM INSIGHTS REPORT

Bromium 脅威情勢レポート 2020 年 3 月

脅威の情勢

Bromium Insights Report は、迫りつつある脅威や兆候にお客様が敏感に気づき、セキュリティチームに対して、現在の攻撃に対処したり、進化する脅威を予測し、自分たちのセキュリティ体制の整備をしたりするのに役立つ知識やツールを提供するために作成されています。

Bromium Secure Platform は、パソコンに導入され、あらゆる潜在的な脅威を隔離された仮想マシンの中に封じ込めた状態で動作させます。 エンドポイントのセキュリティ対策に「隔離」を加えることで、エンドポイントでの防御が最強となり、ネットワークに侵入を試みるどんなマルウェアがあっても、セキュリティチームがこれを監視、追跡、さらに履歴管理することができる、他では得られない利点が得られます。

注目すべき脅威

2020 年 2 月、Bromium 研究部門 は、日本の組織を標的とした Nemty ランサムウェアを配布する大規模で悪意のあるスパム配信活動を観測しました。これによるメールは、悪意のある VBS（VBScript）ダウンローダーを内包した ZIP ファイルを配信していました。Windows Script Host（WScript.exe）で実行すると、VBS ファイルは二種の Nemty ペイロード(攻撃モジュールの実体)のうち 1 つをダウンロードして実行しました。ZIP ファイルは、デジタルカメラで撮影した画像が含まれているとユーザーに思わせるため、カメラファイルシステム（DCF）規格の基準にそって命名されていました。メールの件名は 2 文字または 3 文字の絵文字を含み、受信者の好奇心をそそって開封させるものでした。Nemty の検体は jap.exe および jp.exe という名前が付けられ、日本の組織がこの配信活動のターゲットであったことが示されます。図 2 は、キャンペーンのインフラストラクチャを示しています。赤い点はそれぞれ、Bromium Secure Platform によって隔離された固有の VBS ダウンローダーサンプルを表しています。 3 月に、Nemty の開発者は、身代金要求が支払われなかった場合に被害者から盗んだデータを強要戦術として公に晒しはじめました。

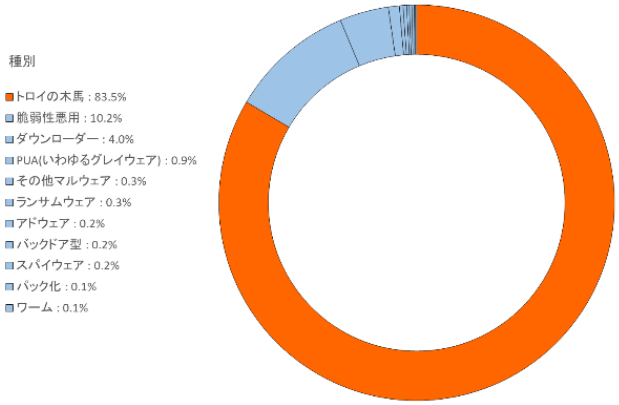

図 1 – マルウェア種類　2020 年 1 月から 2 月

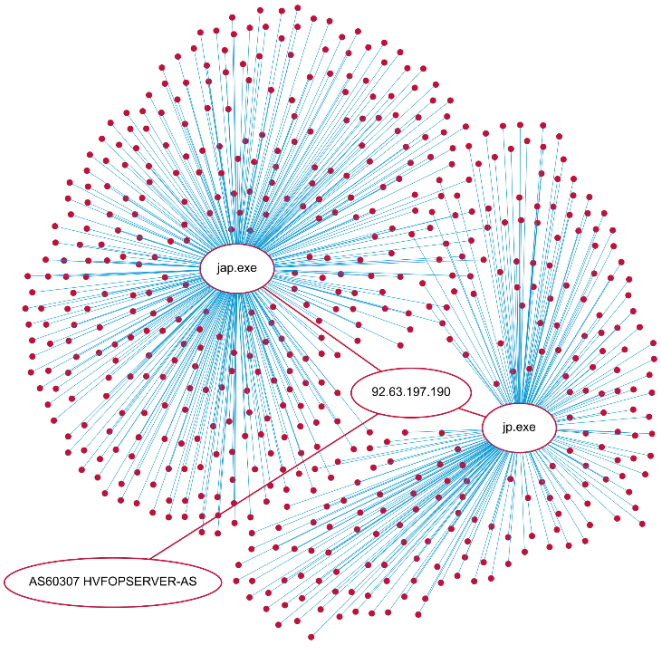

図 2 - Nemty スパム配信活動のインフラ 2020 年 2 月

Bromium 研究部門 は、2020 年 1 月から請求書とされる zip 形式の PDF ファイルを配信する悪意のあるスパム配信活動を特定しました。PDF ファイルには、悪意のある XLS CFBF（Compound File Binary Format）ファイルを選択的に提供する Web ページにつながるハイパーリンクが含まれています。スプレッドシートは Excel の Power Query 機能を使用して、リモートのコマンドアンドコントロール（C2）サーバーからコマンドを取得して実行します。Power Query は、Excel が Web サイトを含むさまざまなソースからデータをインポートできるようにする機能です。スプレッドシートはソーシャルエンジニアリングの画像を利用して、ユーザーを「コンテンツを有効にする」をクリックさせ、その結果、Web クエリがトリガーされます。 Web クエリは攻撃者の C2 インフラストラクチャに接続し、成功すると、C2 サーバーはさまざまなペイロードをダウンロードして実行する一連の Excel 関数で応答します。これまでのところ、コモディティリモートアクセスツール（RAT）と一般に入手可能なシェルコードが配信されていることが確認されています。興味深いことに、シェルコードは calc.exe を起動します。これは、この活動が本番の配信活動の前兆として、外部で機能をテストする攻撃者である可能性を示唆しています。送信者は AOL ウェブメールアドレスで、DKIM および SPF メールチェックにパスしました。執筆時点では、活動は依然進行中です。

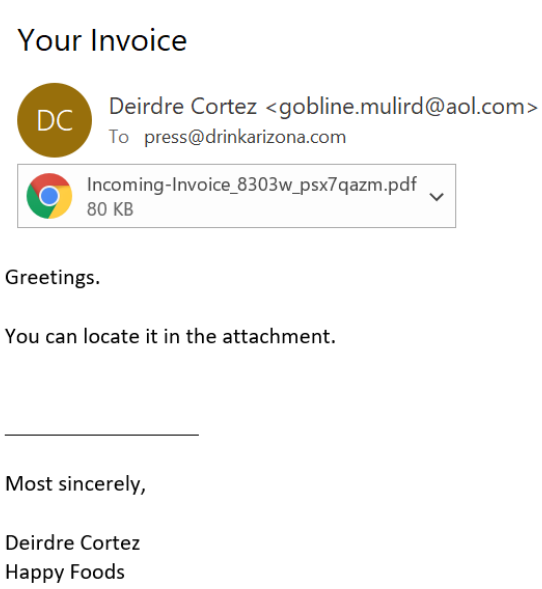

図 3 - 2 月 2 日に送信されたスパムメール

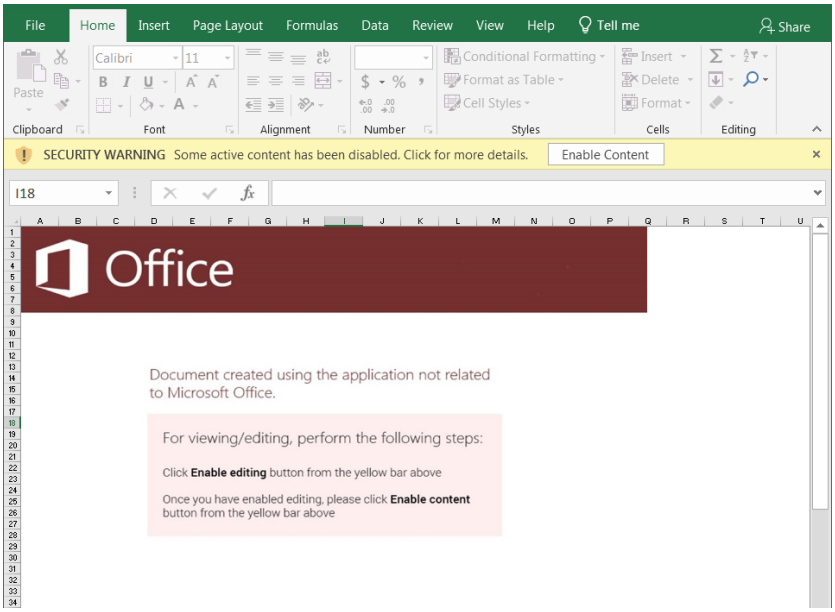

図 4 – 悪意のある IQY クエリを内包した Excel 文書

注目すべき技術

悪意のあるドキュメントには、Microsoft Office の読み取り専用モードの無効化やマクロの有効化などの操作を行うようにユーザーを誘導するために設計された、偽のプログラムプロンプト(訳注:実行を促すメッセージなど)の画像が含まれていることがよくあります。Bromium ブログの脅威調査の投稿で、視覚的類似ドキュメントを含む配信活動の中で分散したマルウェアファミリを追跡し、検出するために、知覚的ハッシュアルゴリズムを使用する方法について説明しています。調査の一環として、ソーシャルエンジニアリングに使用する画像がプログラムで改造されていた QakBot キャンペーンを特定しました。脅威の行為者は、バイナリパディング(T1009)の形式としてランダムな場所に青い楕円を挿入することで各画像を編集していました。これは、画像(および画像を含むドキュメント)が一意のチェックサム値を生成したことを意味します。これは、MD5 などの暗号化ハッシュアルゴリズムの使用で検出を回避するための行為だと考えられます。

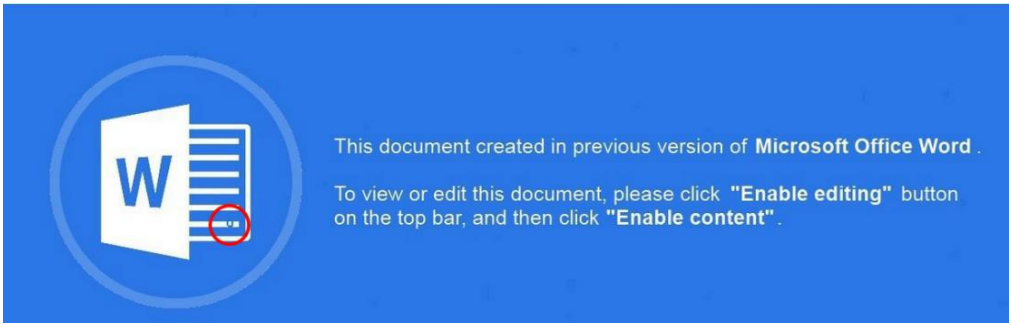

図 5 – ソーシャルエンジニアリングの手口用に偽装された画像(赤丸部分)

既知になった最初の Word マクロウイルス(WM / DMV)が 1994 年に作成されて以来、Office マクロは悪意のあるドキュメントで最も頻繁に使用されるコード実行手法であり続けています[1]。攻撃者の間での頻繁な使用によって、マイクロソフトは長年にわたってセキュリティ制御を導入し、保護されたビュー、信頼できる場所、コード署名などによりコード実行手法としてのマクロの有効性を低下させてきました[2]。しかし、今月の注目すべき脅威のセクションで説明している進行中の悪意のあるスパムキャンペーンでは、攻撃者はコードの実行をマクロに依存していませんでした。その代わり、悪意のある Web クエリ(.IQY)ファイルを作成していました。これは、マクロよりもいくつかの利点がある技術です。図 6 に示すように、Web クエリを使用する悪意のあるドキュメントは検出率が低くなります。これは、受信者がドキュメントを開く前にドキュメントに悪意のあるコードが保存されていないことが一因と考えられます。第 2 に、コマンドは C2 サーバーで提供されるため、攻撃者はパブリック IP アドレスなどのクライアント情報に基づき実行するコマンドを制御して、ターゲット選択を実行できます。

図 6 – コード実行に IQY を使用するスプレッドシートの VirusTotal での認識件数

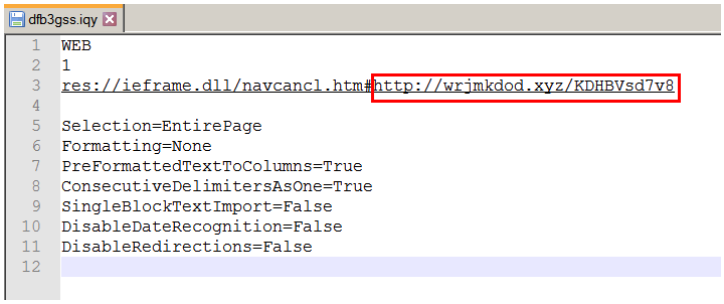

図 7 – 攻撃者の C2 サーバーを示す IQY ファイル内容

すぐに考慮可能な情報

Bromium Secure Platform 推奨事項

マルウェアがホストコンピュータから隔離されており、会社のネットワークに拡散することができないため、Bromium のお客様は常に保護されています。最新の Bromium Secure Platform のソフトウェアリリースに更新しておくこと、また Bromium Controller の Operational and Threat Dashboards を使って、エンドポイントデバイスで隔離が正しく実行されるようにすることをお勧めします。

Bromium の Secure Platform のポリシーでは、メールクライアント用の、信頼されていないファイルの対応と、Microsoft Office の保護オプションを有効にしておく（当社の推奨ポリシーでは、デフォルトで有効）ことをお勧めしています。この設定をオンにしておくことで、フィッシング作戦で感染の危険にさらされる可能性を低減することが簡単にできます。推奨の設定・構成の実装のためにお手伝いできることがあれば、Bromium Support にご連絡ください。

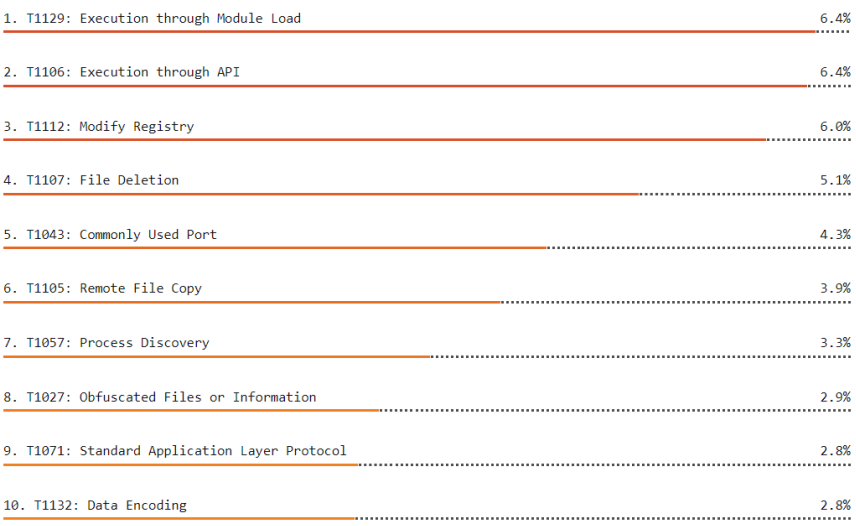

図 8 - MITRE ATT&CK の分類による隔離した脅威の最多 10 種（2020 年 1 月-2 月）

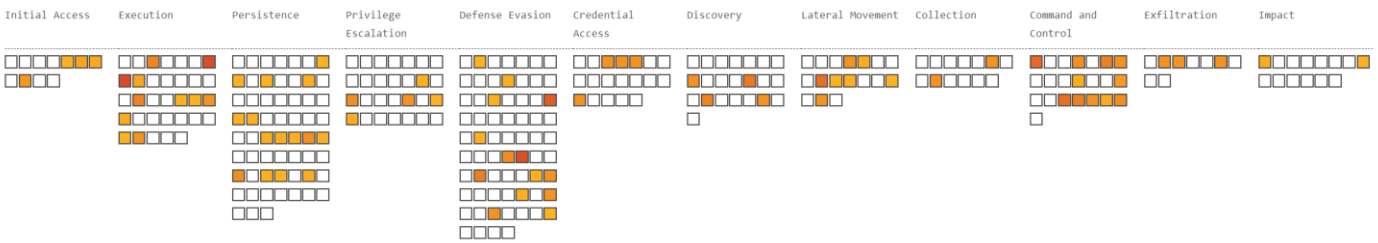

図 9 - 2020 年 1 月-2 月に隔離された脅威が使った手法の分布を表す MITRE ATT&CK ヒートマップ

一般的なセキュリティ推奨事項

詐取された被害者のデータを開示するという Nemty の開発者らの最近の行為は、ランサムウェアファミリー間の最新のトレンドを踏襲しています。2019 年 11 月の Maze 以降、DoppelPaymer や Sodinokibi などのランサムウェアファミリーは、組織に身代金要求を支払うよう圧力をかける同じ戦術を採用しています [3] [4] 。ランサムウェアは、組織のデータの可用性に加えて機密性にもリスクをもたらします。 GDPR などのデータ保護法の違反に対して国内当局が課した罰金で、被害者はさらなる損失に直面する可能性もあります。パッチ管理に関するエンタープライズセキュリティのベストプラクティスに従い、ランサムウェア攻撃の影響をアクセス制御とデータのバックアップで制限できます。

シグネチャー

Bromium 研究部門 は、各セキュリティ担当部署が IQY ファイルを含む疑わしいスプレッドシートを探査するのに使用できる YARA ルールを公開しました。

```
rule hunt_doc_cfbf_iqy {
    meta:
        author = "Bromium Labs"
        date = "2020-03-06"
    strings:
        $magic = {D0 CF 11 E0 A1 B1 1A E1} // Compound File Binary Format header
        $png = {89 50 4E 47 0D 0A 1A 0A} // PNG header of social engineering image
        $jpg = {4A 46 49 46} // JPEG header of social engineering image
        $http = {00 00 68 74 74 70}
        $ref = {00 00 53 68 65 65 74 ?? 21} // Sheet reference to Web Query
    condition:
        $magic at 0 and
        any of ($png, $jpg) and
        $http and
        $ref in (@http..@http + 100) and // Look for $ref within 100 bytes of $http
        filesize < 2000KB
}
```

2020 年 2 月の Nemty 配信活動のメールの添付ファイルは、次の正規表現に従って名前が付けられました。

```
PIC_¥d{6}_2020¥.zip
IMG¥d{6}2020_jpg¥.zip
```

常に最新の状態に

Bromium Insight Report は、Bromium Threat Cloud で脅威対策を共有するよう事前に同意したお客様に対してお送りしています。 私たちに対して送られた警告は、当社のセキュリティ専門家が分析し、偽陽性を減らし、より詳細で信頼性の高い警告に変えます。 また、マイクロ VM で隔離されたマルウェアから収集した脅威データを使って、Bromium によって保護されていない他の重要な資産を守ることもできます。 詳細をお知りになりたい場合は、Threat Sharing の Knowledge Base の記事をご覧ください。

私たちは、導入したものを最大限活用していただけるよう、お客様に次のことをしていただくことをお勧めしています。

- Bromium Cloud Services と Threat Forwarding を有効にする。 これで、お客様のエンドポイントは最新の Bromium の Rules File（BRF）で継続的に更新されるようになり、しかも、お客様に対する最新のセキュリティ侵害について確かな報告ができるようになります。 操作と脅威についての最新情報のレポートのテンプレートを受け取れるよう、最新リリースのたびに Controller を更新するよう設定しておいてください。 最新の リリース通知と、お客様用ポータルで見られるソフトウェアダウンロードをご覧になってください。

- Bromium 研究部門　が追加する、新たに発生した攻撃方法の検出について最新情報を得るため、年に 2 回以上は Bromium のエンドポイントソフトウェアを更新してください。

最新の脅威の調査については、Bromium ブログをご覧になると、新規の脅威について当社の研究者が細かく分析し、その動きについて情報を掲載しています。

出典:

[1] Szor, Peter (2005). The Art of Computer Virus Research and Defense. Addison-Wesley Professional.
[2] https://www.microsoft.com/security/blog/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/
[3] https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/
[4] https://www.bleepingcomputer.com/news/security/nemty-ransomware-punishes-victims-by-posting-their-stolen-data/

Bromium Insight Report について

企業の脆弱性が最も大きくなるのは、ユーザーが電子メール添付を開いたり、電子メールに載っているリンクをクリックしたりすること、またインターネット上のチャットやファイルのダウンロードなどを行うときです。 Bromium Secure Platform は、危険な動作をマイクロ VM の中に閉じ込めて切り離し、マルウェアがホスト PC に感染しないよう、または企業ネットワーク上で拡散しないようにすることで、企業を守ります。 マルウェアが閉じ込められているため、Bromium Secure Platform は、お客様がそのインフラストラクチャ全体を強化するのに役立つ診断データを豊富に集めることができます。 Bromium Insights Report では、報告され、分析された最新の脅威から得られる重大な成果を処理して、お客様が完全に保護されるように努めます。

BROAD 株式会社ブロード
［Company Site］ broad-corp.co.jp
［BROAD Security Square］ bs-square.jp
〒100-0014 東京都千代田区永田町 1-11-30 サウスヒル永田町 7F
TEL：03-6205-7463(代表)
東 京 | 横 浜 | 大 阪 | マレーシア