BROMIUM INSIGHTS REPORT

Bromium 脅威情勢レポート 2019 年 5 月

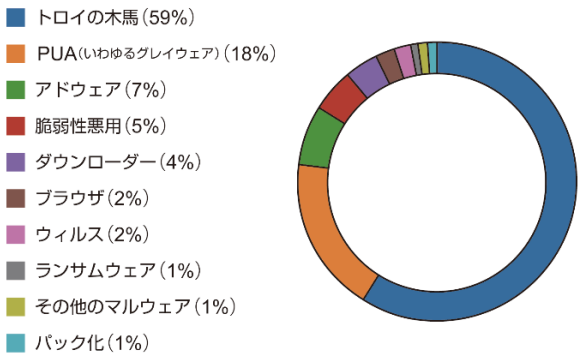
脅威の情勢

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くことができるよう、また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を整えたりできるための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

Bromium の研究所の調査で、米国に置かれた自律システムにあるウェブサーバで、AS53667 と呼ばれるマルウェア配信インフラストラクチャがホストされているのが数週間前に発見されました。攻撃者は、サーバを使って 10 のマルウェアファミリーを、時には同じサーバで複数のファミリーをホストし、これを悪意のスパム作戦を使って配信していたのです。このマルウェアには Dridex、AZORult、GandCrab といったバンキング系のトロイの木馬や情報窃取、ランサムウェアなどがあります。この発見で、マルウェアの操作者が Amazon 形式の在庫・補充最適化サービス（フルフィルメントサービス）を使っていたことが露呈しました。



分類別割合、2019 年 4 月

よく使われるバンキング系のトロイの木馬である Ursnif を配信する作戦は、ステガノグラフィーと呼ばれるデータ埋め込み手法の COM オブジェクトと WMI を使い、セキュリティ制御を回避するなど、次第に高度になっています。こうした作戦は今では位置情報を取得して行われるため、トロイの木馬の操作者が特定の地域や場所を標的にできるようになっています。

Emotet は依然、私たちが隔離した中で最も頻繁に見られる脅威です。このバンキング系トロイの木馬が、保護されていないネットワークでどれほど効果的に足場を作ることができるかを、ブログでの技術分析第 1 部と第 2 部でご覧ください。

注目すべき技術

Visual Basic for Application（VBA）のマクロのようなスクリプト言語（MITRE ATT&CK ID: T1064）を使った実行技術が、4 月に見られた中では最も多かったのですが、これが悪意のペイロードを仕込む方法として唯一のものであるとはとても言えません。私たちが隔離した新種のドロッパーは悪意ある Word 文書に仕込まれており、Windows Explorer のプレビュー画面からプレビューすると、ユーザがファイルを開きもしないうちから、暗号化された PowerShell を実行しました。コマンド実行にユーザの介入を必要としないため、攻撃者は次の攻撃段階を成功させるのにソーシャル・エンジニアリング（人的なセキュリティの排除）に頼る必要がないのです。

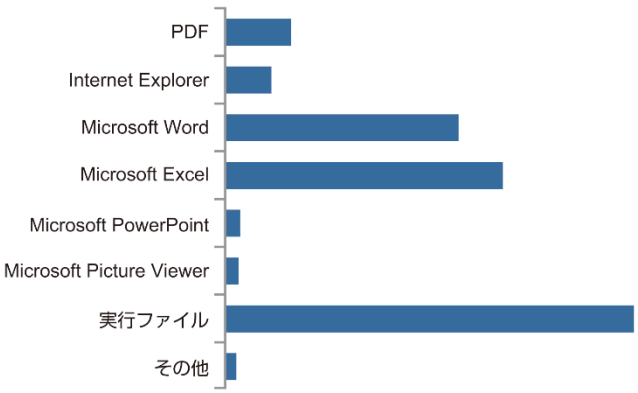
USB ドライブのようなリムーバブル媒体もいまだに、マルウェアを拡散するのに効果的な手段です（MITRE ATT&CK ID: T1091）。私たちはこの 4 月に、感染した USB ドライブが保護されたパソコンに差し込まれた際、悪意のあるショートカット（LNK）ファイルの実行を隔離しました。このドライブにはキー入力監視プログラムや仮想通貨マイニングなどの機能を持ち、AutoIT や AutoHotKey といったスクリプト言語で書きこまれたワームであり、リモートアクセス型トロイの木馬（RAT）でもある Retadup が入っていました。このワームは自ら複製を作り、リムーバブル媒体やネットワーク共有などのファイルシステムの中の、利用可能なすべての領域で増殖します。ショートカットファイルの 1 つが開くと、cmd.exe の処理が増殖し、その後、悪意あるスクリプトを搭載した AutoIT か AutoHotkey の実行ファイルを実行するのです。

すぐに考慮可能な情報

Bromium Secure Platform の推奨事項

マルウェアがホスト PC と分離しており、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。エンドポイントのデバイスで隔離が正しく実行されるようにするため、ソフトウェアのリリースを常に最新のものにしておくことと、Bromium Controller で運用と脅威のダッシュボードを使うようにすることをお勧めします。

実行ファイルの他に、Bromium のお客様全体を通して見られたマルウェアの形式のうち最も多かったのは、ユーザに直接メールを送るか、ウェブブラウザを介してダウンロードするよう誘い込む悪意の Microsoft の Word と Excel の文書です。Bromium Secure Platform のポリシーでは、電子メールクライアントのための信頼できないファイルのサポートと Microsoft Office の保護機能を有効にしておくようおすすめしています（これらは当社の推奨ポリシーによってデフォルトで有効となっています）。こうした設定をオンにしておくことは、フィッシング作戦によって感染するリスクを軽減するための手っ取り早い方法です。



アプリケーション種類別、2019 年 4 月

暗号化された ZIP ファイルで配信された Microsoft Office のマルウェアも若干増えていますが、これは、電子メール添付のスキャンを回避するためによく使われる技法です。この技法の影響を受けにくくするために、私たちは ZIP 保護を有効にしておくことをお勧めします。第 4.1.5 版以降をお使いの場合は、マイクロ VM の中での ZIP ワークフローの使い勝手が非常に向上するという利点もあります。

提案した構成を導入するために、私たちにお手伝いすることがあれば、Bromium にご連絡ください。

一般的なセキュリティ推奨事項

「米国に拠点を置くウェブサーバの集合体がマルウェアをホストしていることがわかった」で判明した重要なことの 1 つは、大規模なフィッシング作戦で配信された Microsoft Office 文書に仕込まれた VBA マクロを使って、ペイロードがダウンロードされたということです。ネットワーク保護のために取れる手段のひとつは、Microsoft Office のマクロ設定をロックダウンして、信頼できるマクロか署名付きのマクロのみが実行できるようにすることにより、マクロのセキュリティのベストプラクティスを追求することです。こうした設定は、導入した Microsoft Office の版に適切な管理者テンプレートを使った Group

Policy を介して強制実行することができます。オーストラリアのサイバーセキュリティセンターが数年にわたって、この課題に対するすぐれたガイダンスを作成しています。さらに、こうした悪意あるスパム作戦につながる実行ファイルのファイル書き込みイベントを検出するために私たちは OpenIOC シグネチャーを提供しています。

シグネチャー

OpenIOC（ロジックツリー）

```
OR
├ File Name is qwerty2.exe
AND
└ File Full Path contains ¥appdata¥local¥temp¥
```

OpenIOC（XML）

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="1f77ee18-7e8f-4d5c-b977-ce1d967483c8"
last-modified="2019-04-15T09:43:09" xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>malware_distribution_servers_dropped_exe</short_description>
  <authored_by>Bromium Labs</authored_by>
  <authored_date>2019-04-12T14:16:05</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="7e582124-e7eb-4b8b-9c9d-fde09f06017d">
      <IndicatorItem id="2a5647a7-0db6-4241-b2f3-5eb29d5c6c54" condition="is">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">qwerty2.exe</Content>
      </IndicatorItem>
      <Indicator operator="AND" id="e2bff2a2-0d37-4794-8b9c-366cef9cd0cf">
        <IndicatorItem id="28205128-91fa-4c7a-b589-60bebb577430" condition="contains">
          <Context document="FileItem" search="FileItem/FullPath" type="mir" />
          <Content type="string">¥appdata¥local¥temp¥</Content>
        </IndicatorItem>
      </Indicator>
    </Indicator>
  </definition>
</ioc>
```

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します。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 社内の Rules File（BRF）が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 release notes と、Customer Portal 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 Labs 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、blog 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。

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 broad-corp.co.jp

本 社 〒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）

大阪営業所 〒531-0072 大阪市北区豊崎 3-4-14 ショーレイビル 6 階
TEL：06-6375-3775（代表）

マレーシアオフィス Block F7-10, Jalan PJU 1a/4 Are Damansare, 47301 Petaling Jaya, Selangor,Malaysia