BROMIUM INSIGHTS REPORT

Bromium 脅威情勢レポート 2020 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、パソコンに導入して、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 3 月から 4 月にかけて、Bromium Lab は新型コロナウイルス（COVID-19）のパンデミックを餌として使い、ユーザーを感染させる脅威の行為者が増加したことを確認しました。フィッシングメールの送り手は通常、ソーシャルエンジニアリングの手法を使って、例えば権威を装ったり、緊急事態だと訴えたり、好奇心をそそったり、めったにない今だけのイベントだと偽ったりして相手をそそのかし、悪意のハイパーリンクや添付ファイルを開かせようとします[1]。
ここ 2 か月間にあった新型コロナウイルス関連のフィッシングメールには、換気装置の発注書や、政府当局からの正式通知、この病気についての新しい治療法に関する安全報告書を騙ったものが特に多く含まれていました。

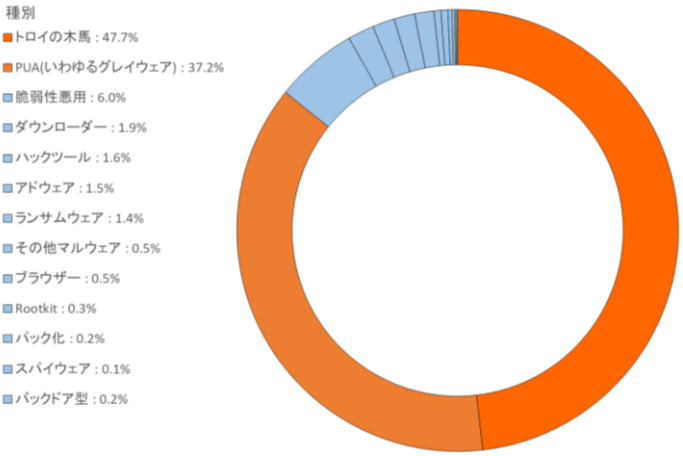

図 1 ―マルウェア種類　2020 年 3 月・4 月

図 2 で示すのはさらに興味深い例で、輸送業界のある組織が、一般に出回っているキー操作監視システムとリモートアクセス型トロイの木馬（RAT）である Agent Tesla を配信するフィッシング詐欺の標的になったものです。メッセージは世界保健機関（WHO）からの正式通知であるように見せかけていました。

図 2 ― HP Sure Controller で見られた新型コロナウイルスのフィッシングメールの例

メールをよりもっともらしく見せるため、攻撃者は WHO のドメインからであるように見える送信アドレスを入れ、CC の欄にも、いかにも法関連の機関であるかのようなメールアドレスを入れていました。標的となった組織のメールのゲートウェイは、Sender Policy Framework （SPF）の認証チェックを構成していたおかげで、送信アドレスが偽物であることを検知したのです。それにもかかわらず、ゲートウェイはこのメールを受信者の受信ボックスに入れてしまい、そこで Bromium(Sure Click)がこれを隔離したのです。

このメールには悪意の Excel スプレッドシートが入っていて、任意コード実行手法を使って Agent Tesla をダウンロードして実行しました。最初の手法は Visual Basic for Applications（VBA）のマクロ自動オープンを介したもので、これはユーザーが「編集を可能にする」と「コンテンツを実行する」をクリックすることで開始されます。ダウンローダーが開始される 2 つ目の方法は、2018 年 1 月のアップデート公開前のバージョンにあった Microsoft Office の Equation EditorCVE-2017-11882 という脆弱性を利用したものでした[2]。

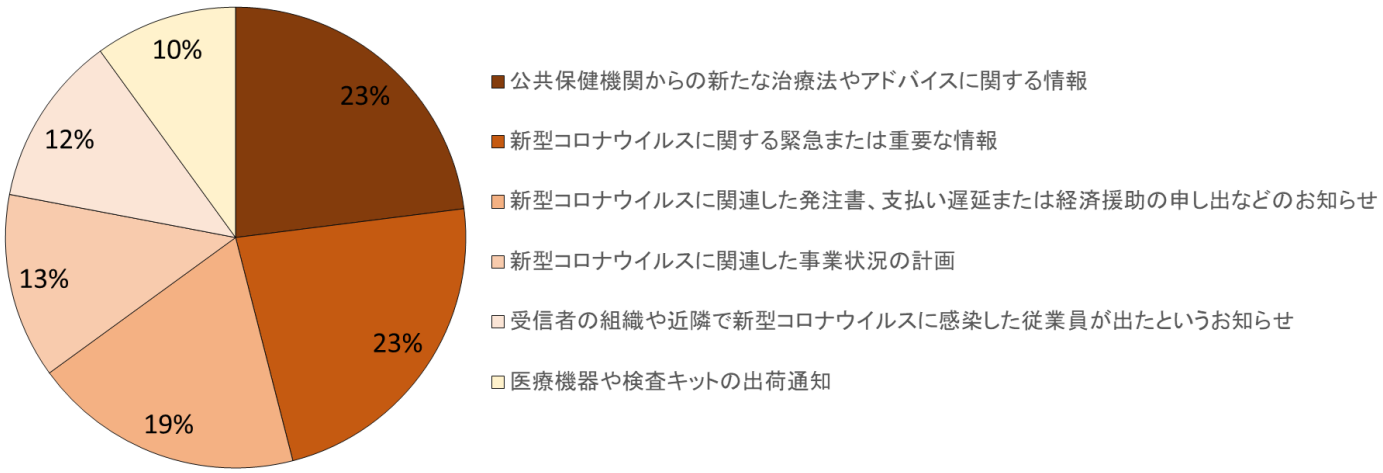

図 3 — 2020 年 3 月と 4 月に Bromium(Sure Click)で隔離された新型コロナウイルス関連の脅威で使われたメールの餌

Maze ランサムウェア

4 月 18 日、米国の IT サービス会社、Cognizant は、同社の社内システムがランサムウェアに感染し、一部の顧客へのサービスに支障が出ていると発表しました[3]。同社はこの侵入を行ったランサムウェアシリーズが Maze であると特定しました。Maze の背後で暗躍するのは、最近活動中の非常に大胆なランサムウェアの使用者です。2019 年 11 月に発足し、詐取した被害者のデータを公開し、企業に身代金を支払わせるゆすりの材料として使った最初のグループで、その後、ほかのマルウェア作成者もこれを使用しました[4]。この開発者はマルウェア調査団体を注意深く監視し、そのマルウェアの公開分析に迅速に反応しました。Maze が関連する過去の事件では、盗んだリモートアクセスサービス（RAS）の認証情報や悪意のメール添付、Fallout や Spelevo エクスプロイトキットを使った配信など、さまざまな攻撃経路と方法を使っていました[5]。攻撃者はまた、自分たちの身代金要求の交渉に応じなければ、ウェブサイトを立ち上げて盗んだ被害者のデータを晒したり、被害者が非難されるような声明を公開するなどとしています。（図 4）。

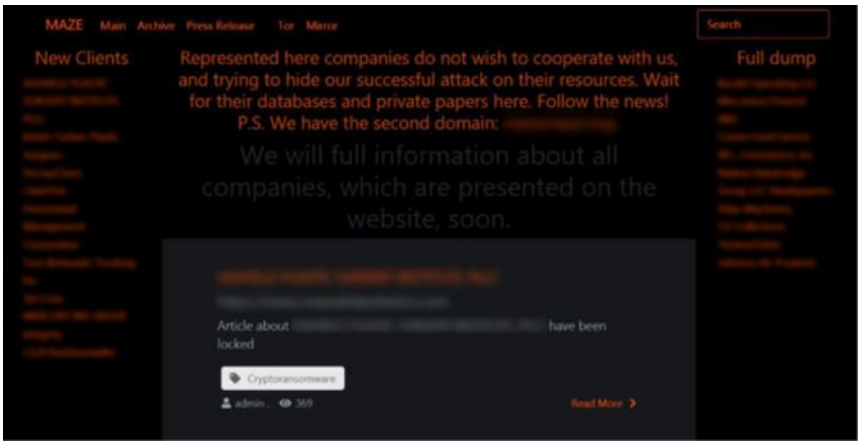

図 4 — 2020 年 5 月、Maze のオペレータが実行すると宣言したウェブサイト

注目すべき技術

暗号化された文書と「デフォルト」のパスワードを使った検出回避

脅威の実行者は静的な検出を避けるために暗号化された文書を使うことが多いものです。この手法における一つの制限は、攻撃者が標的のユーザーにパスワードと文書の復号化方法を伝えなければならず、これにより疑いを招くかもしれないことです。攻撃者にとって都合のいいことに、多くの文書標準には、ユーザーがファイルを開く以外に何の手も加えずに、暗号化された文書を復号化できるようにする、あまり言及されず知られていない機能があるのです。たとえば、Microsoft Excel のバイナリファイル形式（.XLS）ではワークシートを暗号化できます。暗号化されたワークシートのキーに”VelvetSweatshop”が設定されていれば、Excel はユーザーに、文書を開くときにパスワードを入れるように指示しなくても自動的にこのワークシートを復号化するのです[6]。図 5 は、Ursnif と QakBot のバンキング系トロイの木馬を配信した 2020 年 4 月の事件で、悪意の XLS ファイルを復号化した例を示しています[7][8]。

ポータブル・ドキュメント・フォーマット（PDF）もまた、ユーザーと所有者のパスワードで文書にパスワード保護をかけることができるようにした仕様です[9]。ユーザーのパスワード文字数がゼロのキーに設定されていれば、Adobe Reader はユーザーが文書を開いたときに指示することなく自動的にその文書を復号化します[10]。これが意味することは、PDF ファイルを開くときにユーザーが操作する必要なく復号化できるような悪意の暗号化 PDF ファイルを攻撃者が作成でき、それによって静的な分析を回避できるということです。図 6 は、QPDF を使ってユーザーのパスワードが空白のまま暗号化された PDF ファイルを特定し、復号化する方法を示しています[11]。

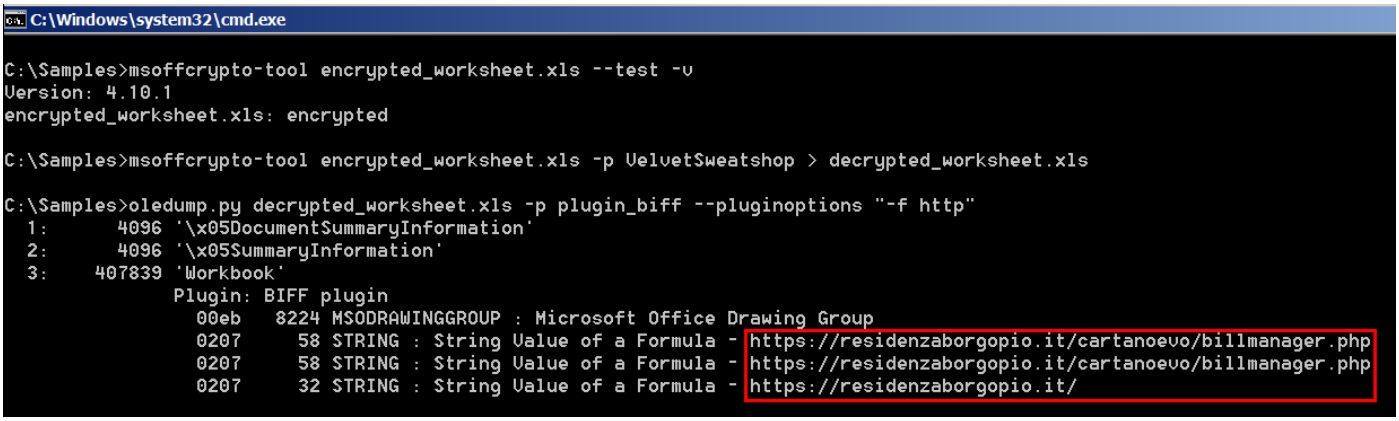

図 5 — "VelvetSweatshop"キーを使って暗号化した悪意の XLS ワークシートの復号化。
バンキング系トロイの木馬をホストしていた配信サーバが赤くハイライトされている。

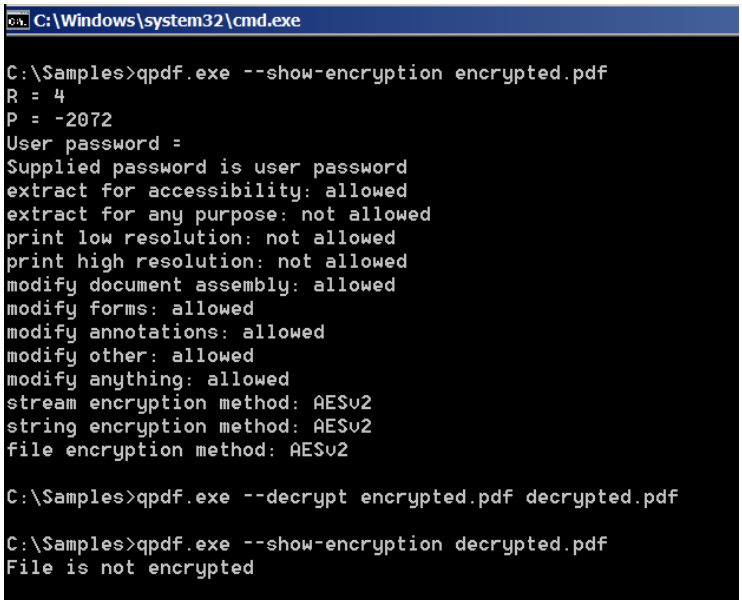

図 6 — 長さゼロのパスワードを使って暗号化された PDF ファイルの復号化

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。

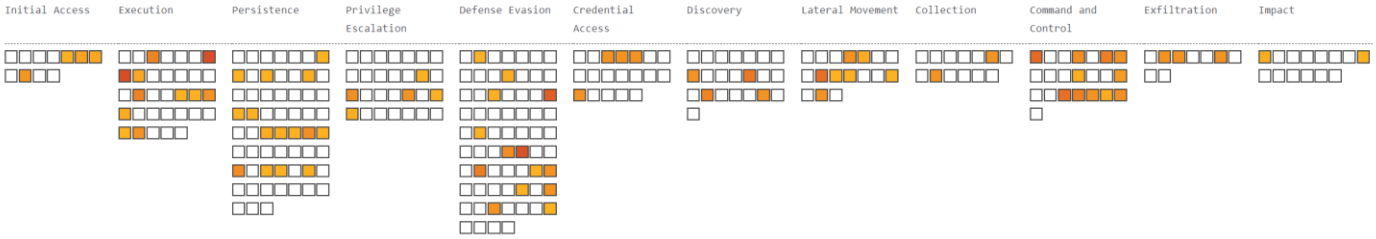

図 7 — 隔離された脅威が使った手法の分布を表す MITRE ATT&CK ヒートマップ(2020 年 3 月と 4 月)

一般的なセキュリティ推奨事項

新型コロナウイルスの世界的流行に伴って、遠隔会議用や RAS、バーチャル・プライベート・ネットワーク（VPN）のソフトウェアなど、在宅勤務で使用される技術を悪用しようとする攻撃者が増えています。今月の「注目すべき脅威」の項にもあるように、マルウェアを配信するために使われた新型コロナウイルス関連のフィッシング詐欺も増えています。4 月には、英国の国立サイバーセキュリティセンター（NCSC）と米国のサイバー・インフラ安全保障局（CISA）が共同で新型コロナウイルス関連の脅威について勧告を発表しました[12]。企業組織は VPN を安全に構成する、ソフトウェアパッチを速やかにインストールするなどといった、NCSC と CISA が定めるガイドラインに従うことで、リスクを減らすことができるのです。

図 8 — 隔離した脅威の MITRE ATT&CK の定義による最多 10 種 (2020 年 3 月と 4 月)

シグネチャー

Bromium Lab は、暗号化されたワークシートの入っている疑わしい XLS ファイルを検出するためにセキュリティチームが使うことのできる YARA 規則を公開しました。

```
rule hunt_xls_encrypted_worksheet {
  meta:
    author = "Bromium Labs"
    date = "2020-04-17"

  strings:
    $magic = {D0 CF 11 E0 A1 B1 1A E1}
    $csp_mscrypto = "Microsoft Enhanced Cryptographic Provider v1.0" wide

  condition:
    $magic at 0 and
    $csp_mscrypto in (0..1000) and
    filesize < 10000KB
}
```

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]https://www.ncsc.gov.uk/guidance/suspicious-email-actions
[2]https://support.office.com/en-gb/article/equation-editor-6eac7d71-3c74-437b-80d3-c7dea24fdf3f
[3]https://news.cognizant.com/2020-04-18-cognizant-security-update
[4]https://www.bleepingcomputer.com/news/security/nemty-ransomware-punishes-victims-by-posting-their-stolen-data/
[5]https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze
[6]https://www.mimecast.com/blog/2020/03/velvetsweatshop-microsoft-excel-spreadsheet-encryption-rises-again-to-deliver-limerat-malware/
[7]https://github.com/nolze/msoffcrypto-tool
[8]https://blog.didierstevens.com/programs/oledump-py/
[9]https://en.wikipedia.org/wiki/PDF#Security_and_signatures
[10]https://www.synack.com/blog/decrypting-malicious-pdf-documents-part-one/
[11]http://qpdf.sourceforge.net/
[12]https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf

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。

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