BROMIUM INSIGHTS REPORT

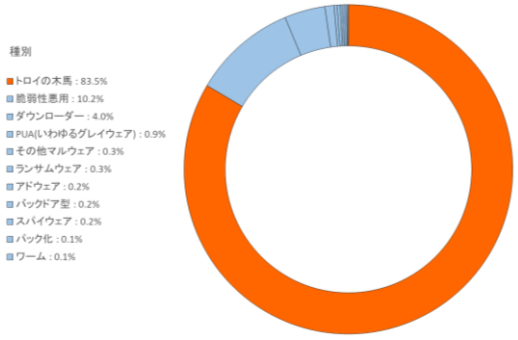
Bromium 脅威情勢レポート 2019 年 11 月

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。

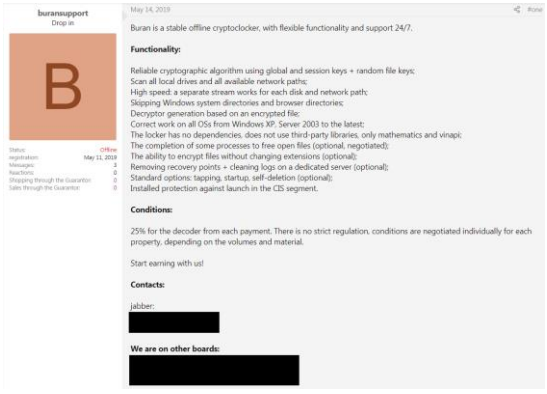
Bromium Secure Platform は、パソコンに導入され、あらゆる潜在的な脅威を隔離された仮想マシンの中に封じ込めた状態で動作させます。 エンドポイントのセキュリティ対策に「隔離」を加えることで、エンドポイントでの防御が最強となり、ネットワークに侵入を試みるどんなマルウェアがあっても、セキュリティチームがこれを監視、追跡、さらに履歴管理することができる、他では得られない利点が得られます。

注目すべき脅威

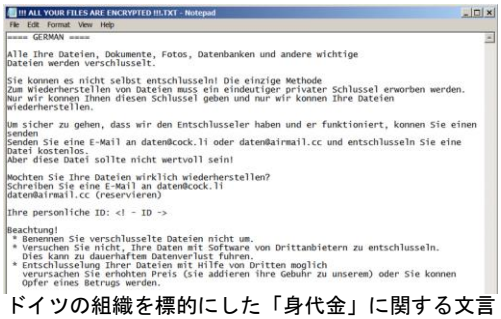


マルウェアのコマンド&コントロール（C2）インフラストラクチャが 2019 年 8 月 22 日にオンラインと認識された後の同年 9 月 16 日、大量の Emotet を使った悪意のスパム配信が再開されました。Emotet スパムの活動は、同年 6 月初めから停止していました。Bromium Lab は新たな侵害活動を分析し、Emotet によるシステムの感染の方法に現われた変化について文書にしました。注目すべき変化は、異なるパッカーや MIME の種類、ひっかけ文句などにあります。また同年 9 月には、Emotet のペイロードをダウンロードして実行する、JScript ダウンローダーの使用の拡散も見られました。これまで、Emotet の制御者は、マルウェアのダウンロードに PowerShell のダウンロード・クレイドル（訳注、通常パラメータを含めた 1 行のコマンド）を使っていました。Bromium Lab は、更新された JScript ダウンローダーについて詳細に分析しました。

2019 年 10 月初め、ドイツで複数の組織が Buran というランサムウェアを配信する悪意のスパム侵入の標的となりました。Buran は市販されているランサムウェアの一種で、2019 年 5 月にロシア語圏のフォーラムで広告が発見されています。Buran の開発者はこのランサムウェアを、サービスとしてのランサムウェア（RaaS）の計画の一部として、見込み顧客である運用（制御）者に販売し、被害者がファイルの復号化に使われる「復号キー」と引き換えに出費する身代金から 25%を受け取ります。この事件では、eFax と呼ばれる合法のオンライン・ファックスサービスからのメッセージを装ったメールが使われました。このメールは、添付ファイルがないため、メール・ゲートウェイのセキュリティ機構を回避することに成功したのです。Buran のアフィリエイトが 24 の eFax のタイポスクワット（スペルミスを利用した不正）のドメインを登録し、そこで悪意の Microsoft Word 文書を設置しました。文書を開くことで Visual Basic for Applications（VBA）の AutoOpen マクロの実行が開始されて、ランサムウェアがダウンロードされます。Bromium Lab がこのマルウェアを分析したところ、Buran のバージョン 5 が配信されていることがわかりました。



2019 年 5 月の Buran アフィリエイト計画に関する広告の英訳



ドイツの組織を標的にした「身代金」に関する文言

```
db 'QUICK >>> UNDECRYPTABLE >>> ENCRYPTING RANDOM FILEBLOCKS /// THIS'
db ' IS BURAN /// GENERATION V',0
```

Buran の実行ファイルで認識された
バージョン 5 のシグネチャー文字列

Bromium Lab は先月、スクリプトベースの 2 種類のマルウェア、JasperLoader と FTCODE も分析しました。JasperLoader は VBScript で書かれた軽量のローダーで、FTCODE ランサムウェアをダウンロードして実行する際に使われたものです。ランサムウェアシリーズの中でも FTCODE の注目すべき点は JasperLoader のように、コンパイルされたプログラミング言語で書かれていないからです。FTCODE は PowerShell で書かれているのです。この侵入作戦はイタリア語話者を狙ったもののようです。ひっかけ文句がイタリア語であったためです。OS など既存の環境に寄生することで、Windows Script Host（WScript.exe）のようなバイナリや、実行用の PowerShell、スクリプトベースのマルウェアなどは、リスクの高い OS ユーティリティの使用が制限されておらず、監視もされていない環境では検出の回避が可能です。

注目すべき技術

文字の難読化（T1027）は、インタープリタ言語で書かれたマルウェアの検出されることを回避するために通常使用される手法です。Emotet の JScript ダウンローダーにも、さらに 2 つの解析（分析）妨害の対策が取られていました。1 つ目は、スクリプトのコンソール出力機能の出力レベル「情報」、「デバッグ」や「証跡」など、あらゆる監査レベルを定義し直すことで、このスクリプトの影響に関するコンソール出力監視を妨害します。これにより、ステートメントや変数の難読化解除された値が実行後に出力される事が妨害されます。2 つ目は無名関数テンプレートの使用で、これはスクリプトのデバグを無効にする働きをします。例えばマルウェア解析者がブラウザを使ったりしてスクリプトのデバッグを試みても、保護機能の影響で、削除されるまでデバッガーをフリーズさせてしまうのです。

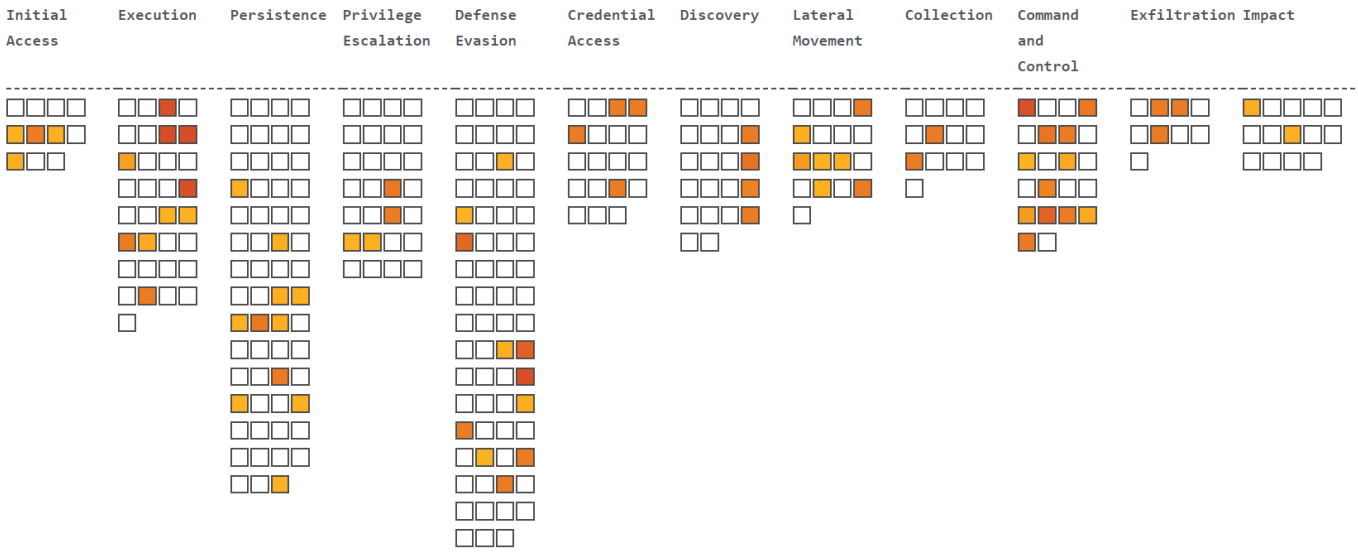
```
    case '1':
        if (!ay["console"]) {
            ay["console"] = function(am) {
                var an = "0|6|5|8|7|1|2|3|4"["split"]('|'),
                    ao = 0x0;
                while (!![]) {
                    switch (an[ao++]) {
                        case '0':
                            var a7 = {};
                            continue;
                        case '1':
                            a7["error"] = am; //am = {}
                            continue;
                        case '2':
                            a7["exception"] = am;
                            continue;
                        case '3':
                            a7['trace'] = am;
                            continue;
                        case '4':
                            return a7;
                        case '5':
                            a7["warn"] = am;
                            continue;
                        case '6':
                            a7["log"] = am;
                            continue;
                        case '7':
                            a7["info"] = am;
                            continue;
                        case '8':
                            a7["debug"] = am;
                            continue;
                    }
                    break;
                }
            }(as);
```

値が 1 の場合の switch のステートメントが[“console”][“LEVEL”]を、空の関数「am」に定義し直している

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。



2019 年 10 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

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。

MITRE ATT&CK の分類による隔離した脅威の最多 10 種（2019 年 10 月）

一般的なセキュリティ推奨事項

ランサムウェアの攻撃は依然、企業に多大なリスクを負わせています。2019 年 10 月 2 日、連邦捜査局は公共広告の中で、無差別的なランサムウェアのインシデント数は 2018 年から減っている一方、ランサムウェアによる損失の総額は増えていると述べています。パッチ管理やアクセス制御、データのバックアップなど、企業セキュリティのベストプラクティスを実践することで、こうした攻撃の影響を抑えることができるのです。

シグネチャー

Buran ランサムウェアをダウンロードするのに使われた悪意の文書には、それぞれジャンクデータを含む 4 つの XML ファイルが含まれていました。このジャンクデータの目的はおそらく、文書のファイルサイズやハッシュを変え、こうした属性を元にした検出を回避するためでしょう。この攻撃の文書構成要素を検出する YARA 規則を以下の通り記載します。

```
rule doc_efax_buran {
  meta:
      author = "Bromium Labs"
      date = "2019-10-10"
      sample_1 = "7DD46D28AAEC9F5B6C5F7C907BA73EA012CDE5B5DC2A45CDA80F28F7D630F1B0"
      sample_2 = "856D0C14850BE7D45FA6EE58425881E5F7702FBFBAD987122BB4FF59C72507E2"
      sample_3 = "33C8E805D8D8A37A93D681268ACCA252314FF02CF9488B6B2F7A27DD07A1E33A"
  strings:
      $vba = "vbaProject.bin" ascii nocase
      $image = "image1.jpeg" ascii nocase
      $padding_xml = /[a-zA-Z0-9]{5,40}¥d{10}¥.xml/ ascii
  condition:
      all of them and filesize < 800KB
}
```

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
［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