BROMIUM INSIGHTS REPORT

Bromium 脅威情勢レポート 2019 年 9 月

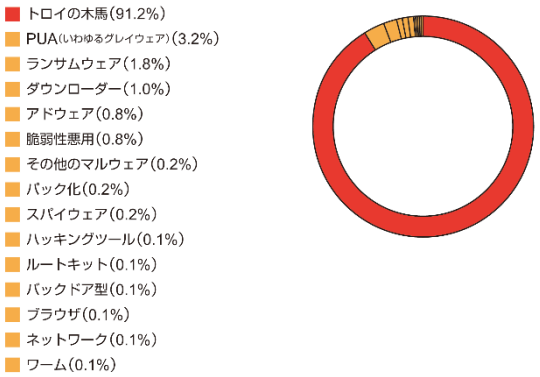
脅威の情勢

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

Emotet のコマンド&コントロール（C2）インフラストラクチャが 8 月 22 日、2019 年 6 月初めからの長い休眠期間を経て、オンラインに戻ってきたことが確認されました。この記事を書いている時点では、新たな悪意のスパム攻撃はまだ確認されていませんが、ボットネットの再開は、新たな攻撃の先駆けのように思えます。



マルウェア 分類別割合、2019 年 8 月

8 月、Bromium Lab は、大変興味深い解析妨害機能を内蔵したドロッパーを解析しました。このマルウェアは、メモリがマップされた ntdll.dll、つまりユーザモードのシステムコールが入っているダイナミックリンクライブラリを改ざんしてフック API を削除することで、検出を回避しようとしました。API のフックは悪意の行為を検出して遮断するためにエンドポイント検出応答（EDR）ツールでよく使われています。このドロッパーは最終的に、一連の身元証明書窃取のマルウェアである Agent Tesla を配信しました。

8 月初め、TrickBot の操作者は、市販されている JavaScript （より具体的には JScript ）のダウンローダーである Ostap を使い始めました。 以前は、フィッシング攻撃は難読化されたコマンドシェル（cmd.exe）と、Visual Basic for Applications（VBA）マクロによって自動的に起動する PowerShell コマンドを使ったダウンローダーをもっぱら利用して、TrickBot ペイロードを配信していました。Ostap は、検出率が低く、サイズが大きく、かなり優秀な解析妨害機能があることで知られています。 Bromium Lab は、このダウンローダーの難読化解除の方法を段階的に記載した「Ostap の難読化解除」についてブログ投稿し、難読化解除を自動化するツールも発表しました。

7 月、私たちは、バンキング系トロイの木馬 Dridex の新しい亜種を配信するフィッシング攻撃を確認しました。この亜種がよく知られているのは、下記のように検出を避けるための 5 つのコード挿入手法を使っているからです。

- AtomBombing
- DLL order hijacking
- Process hollowing
- PE injection
- Thread execution hijacking

Bromium Lab のブログ投稿、「Dridex’s Bag of Tricks」では、Dridex がそれぞれの手法を使って目的を達する方法について解説しています。

2 部構成のブログ、「L0rdix RAT Panel と Builder の分析」と、「L0rdix RAT の C2 の解読」で、Bromium Lab は、地下フォーラムで出回っている.NET リモートアクセスのトロイの木馬（RAT）である L0rdix のボット、ビルダー、ウェブパネルの不正なコピーを分析しました。L0rdix の C2 トラフィックを暗号化するために使われるデフォルトの AES キーがパネルで見つかり、Bromium Lab はパケットキャプチャから L0rdix のトラフィックを解読するツールについて書きました。

```php
define(KEY, "3sc3RLrpd17");  <-- Default C2 encryption key

function decrypt($encrypted){
    $method = 'aes-256-cbc';

    $encrypted = str_replace("~", "+", $encrypted);
    $password = substr(hash('sha256',  KEY ,true), 0, 32);

    $iv = chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0)
     . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0);


    $decrypted = openssl_decrypt(base64_decode($encrypted), $method, $password,
    OPENSSL_RAW_DATA, $iv);
    return $decrypted;
}
```

デフォルトのキーを含め、L0rdix の C2 トラフィックの解読に使われた PHP 関数

Bromium Lab は、韓国語圏の組織を標的とした攻撃で注目を浴びた RAT、FlawedAmmyy の新しい亜種について、また、Bromium Secure Platform が検出前の防御手段を使って、どのようにこうした攻撃をかわすかという方法についても分析しました。

注目すべき技術

Agent Tesla を配信したドロッパーが使用した API アンフック技術は、興味深い形の防衛回避（TA0005）です。このドロッパーは、次の手順を実行してフックされた API を削除するシェルコードを内蔵しています。

1. シェルコードが、NtProtectVirualMemory の呼び出しを使って、ntdll.dll のメモリアクセス許可を PAGE_EXECUTE_READWRITE に変更します
2. Wow64Transition の値がある場所の前、フックが置かれるはずの 5 バイトを上書きして、API フックを削除します。5 バイト以下のサイズのフッキング命令は、もともとそこにあった命令に置き換えられます。
3. シェルコードはその後、その領域のページアクセス許可を PAGE_EXECUTE_READ に戻し、ShellExecuteW の呼び出しでペイロードを開始します。

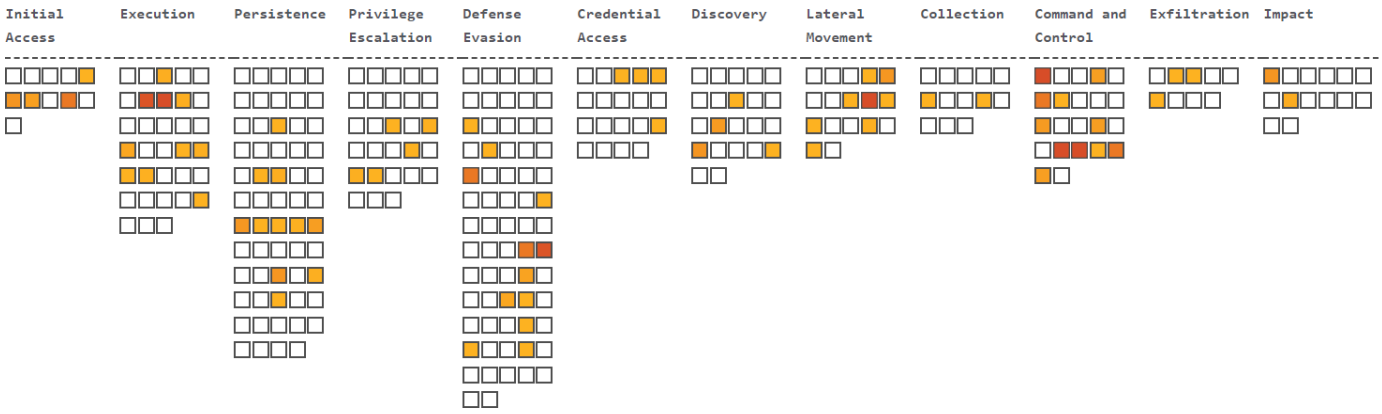
```
004A0A4A   B8 01000000     mov   eax,1
004A0A4F   41              inc   ecx
004A0A50   43              inc   ebx
004A0A51   813B 50C39090   cmp   dword ptr ds:[ebx],9090C350
004A0A57   75 12           jne   4A0A6B
004A0A59   C603 BA         mov   byte ptr ds:[ebx],BA
004A0A5C   8953 01         mov   dword ptr ds:[ebx+1],edx
004A0A5F   8943 FC         mov   dword ptr ds:[ebx-4],eax
004A0A62   C643 FB B8      mov   byte ptr ds:[ebx-5],B8
004A0A66   40              inc   eax
004A0A67   41              inc   ecx
004A0A68   43              inc   ebx
004A0A69   EB 0C           jmp   4A0A77
004A0A6B   3B13            cmp   edx,dword ptr ds:[ebx]          edx = 77BC2430
004A0A6D   75 08           jne   4A0A77
004A0A6F   8943 FB         mov   dword ptr ds:[ebx-5],eax
004A0A72   C643 FA B8      mov   byte ptr ds:[ebx-6],B8
004A0A76   40              inc   eax
004A0A77   803B E8         cmp   byte ptr ds:[ebx],E8
004A0A7A   75 25           jne   4A0AA1
004A0A7C   837B 01 00      cmp   dword ptr ds:[ebx+1],0
004A0A80   75 1F           jne   4A0AA1
004A0A82   8943 FC         mov   dword ptr ds:[ebx-4],eax
004A0A85   C643 FB B8      mov   byte ptr ds:[ebx-5],B8
004A0A89   40              inc   eax
004A0A8A   51              push  ecx
004A0A8B   31C9            xor   ecx,ecx
004A0A8D   43              inc   ebx
```

API フックを削除する、Agent Tesla のドロッパー内のシェルコード（2019 年 8 月）

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 8 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 のポリシでは、電子メールのクライアント用の信頼されていないファイルのサポートと、Microsoft Office の保護オプションを有効にしておく(私たちの推奨ポリシでは、デフォルトで有効になっています)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は、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くすることが簡単にできます。提案された構成を導入するためにお手伝いすることがあれば、Bromium Support にご連絡ください。

1. T1129: Execution through Module Load
2. T1043: Commonly Used Port
3. T1071: Standard Application Layer Protocol
4. T1106: Execution through API
5. T1112: Modify Registry
6. T1105: Remote File Copy
7. T1195: Supply Chain Compromise
8. T1107: File Deletion
9. T1036: Masquerading
10. T1132: Data Encoding

隔離した脅威の MITRE ATT&CK の定義による最多 10 種(2019 年 8 月)

一般的なセキュリティ推奨事項

お客様の企業で、望ましくないと思われるアプリケーション(Potentially Unwanted Application)の利用を追跡すると、以前に発生したデータ流出の道の経路がわかるかもしれません。例えば、多くのサードパーティソフトウェア会社が、Bomgar や TeamViewer などの合法なリモートアクセスのソフトウェアを使って自社製品の遠隔サポートを行っています。合法ではあっても、このようなアプリケーションは悪意の目的で利用されることもあるので、通常は PUA に分類されます。企業内でリモートアクセスソフトウェアの使用履歴を追跡し、承認を得た使用であることを確認するようお勧めします。

シグネチャー

今月のシグネチャーで注目すべきは、Ostap と L0rdix のマルウェアの検出方法です。下記に、このシリーズを検出するための YARA 規則を記載します。L0rdix の C2 トラフィックの解読と、Otap の難読化解除を自動化するための Python スクリプトも、GitHub からダウンロードして入手できます。

```
rule win_ostap_jse {
  meta:
    author = "Alex Holland @cryptogramfan (Bromium Labs)"
    date = "2019-08-29"
    sample_1 = "F3E03E40F00EA10592F20D83E3C5E922A1CE6EA36FC326511C38F45B9C9B6586"
    sample_2 = "38E2B6F06C2375A955BEA0337F087625B4E6E49F6E4246B50ECB567158B3717B"
  strings:
    $comment = { 2A 2A 2F 3B } // Matches on **/;
    $array_0 = /¥w{5,8}¥[¥d+¥]=¥d{1,3};/
    $array_1 = /¥w{5,8}¥[¥d+¥]=¥d{1,3};/
  condition:
    (($comment at 0) and (#array_0 > 100) and (#array_1 > 100)) or
    ((#array_0 > 100) and (#array_1 > 100))) and
    (filesize > 500KB and filesize < 1500KB)
}
```

```
rule win_lOrdix {
  meta:
    author = "Bromium Labs"
    date = "2019-07-19"
    sample_1 = "18C6AAF76985404A276466D73A89AC5B1652F8E9659473F5D6D656CA2705B0D3"
    sample_2 = "C2A4D706D713937F47951D4E6E975754C137159DC2C30715D03331FC515AE4E8"
  strings:
    $ua = "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0" wide //
Firefox 53 on Windows 10
    $sig = "LOrdix" wide ascii
    $sched_task = "ApplicationUpdateCallback" wide
    $exe = "syscall.exe" wide
    $cnc_url_1 = "connect.php?" wide
    $cnc_url_2 = "show.php" wide
    $browser_1 = "¥¥Kometa¥¥User Data¥¥Default¥¥Cookies" wide
    $browser_2 = "¥¥Orbitum¥¥User Data¥¥Default¥¥Cookies" wide
    $browser_3 = "¥¥Amigo¥¥User¥¥User Data¥¥Default¥¥Cookies" wide
    $coin_regex_1 = "[13][a-km-zA-HJ-NP-Z1-9]{25,34}" wide // Bitcoin
    $coin_regex_2 = "0x[a-fA-F0-9]{40}" wide // Ethereum
    $coin_regex_3 = "L[a-zA-Z0-9]{26,33}" wide // Litecoin
  condition:
    uint16(0) == 0x5A4D and (any of ($ua,$sig,$sched_task,$exe)) and (any of ($cnc_url_*))
and (any of ($browser_*)) and (any of ($coin_regex_*))
}
```

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