BROMIUM INSIGHTS REPORT

Bromium 脅威情勢レポート 2019 年 7 月

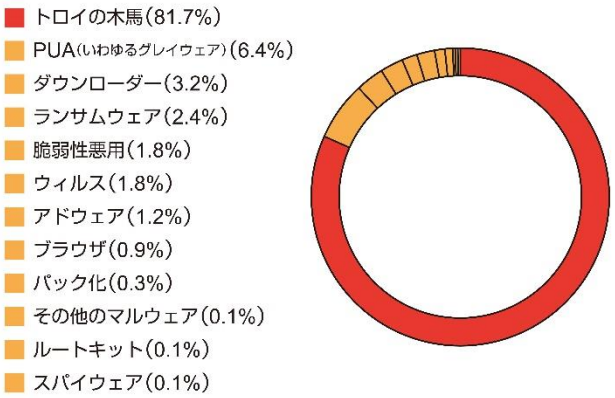
脅威の情勢

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。

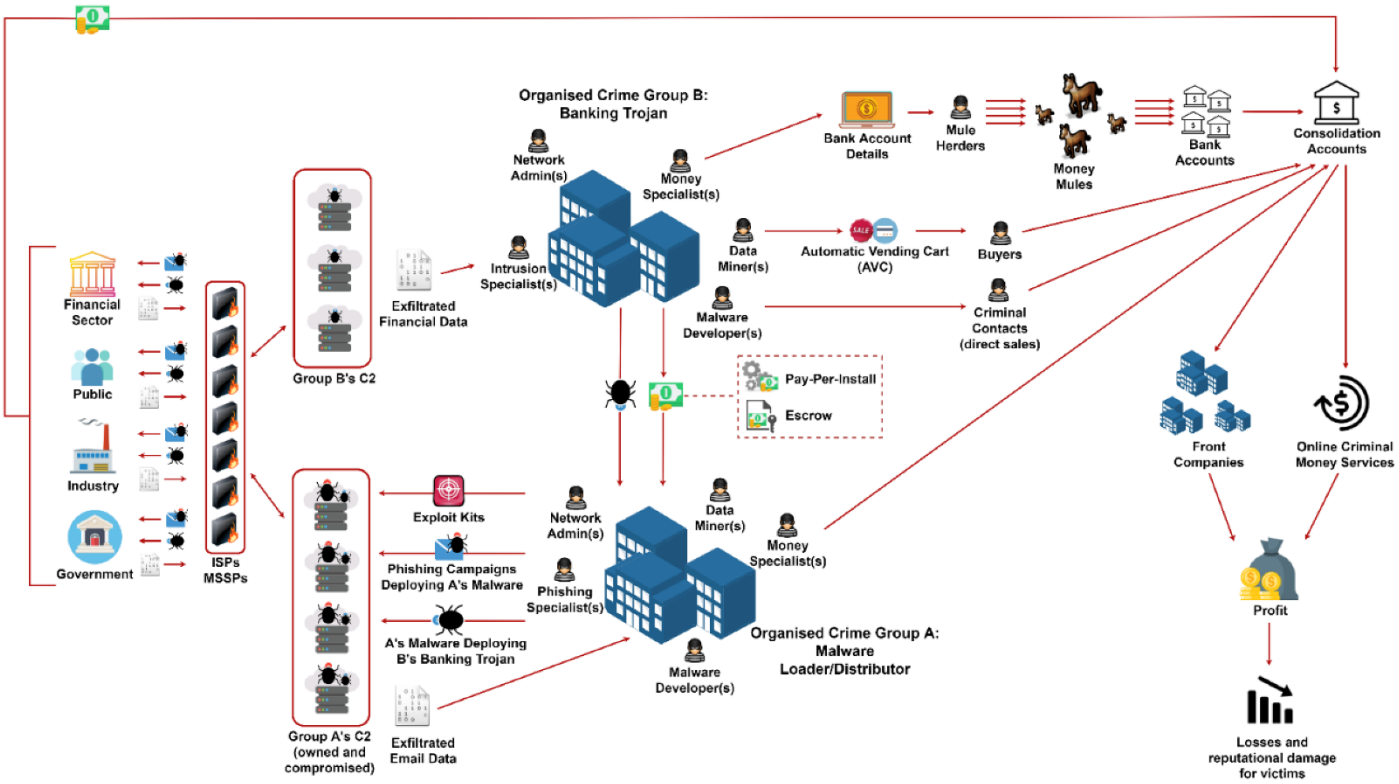
注目すべき脅威

フロリダにある 2 つの都市、Riviera Beach と Lake City は、ランサムウェアに侵入された後、総額 110 万（米ドル）の身代金を支払いました。 Lake City の市当局は、「三段攻撃」の標的にされた経緯を説明しましたが、これはおそらく、Emotet の感染に続いて TrickBot による Ryuk ランサムウェアが配信されたことについて述べたものだと思われます。 こうしたインシデントによって、データへのアクセスを取り戻すために身代金を払う犠牲者の倫理的、実務的な問題が浮き彫りになっています。 Lake City については、身代金の費用はサイバー責任保険で賄われましたが、このようなタイプの保険は、1930 年代に設定された幼児誘拐と身代金（K&R）保険を模したもので、近年人気が高まっています。 犠牲者にとって、身代金を支払う方が、費用も時間も多くかかる修復プロジェクトを選択するよりも — とりわけバックアップを取っていない場合には — 利己的ではあっても魅力的な手段なのです。 例えば、2019 年 3 月に起こり、Norsk Hydro が被害を受けた LockerGoga のランサムウェアの修復費用は 5200 万ドルだったと言われています。 しかし、身代金を支払えば、犯罪グループの活動に資金を提供することになり、攻撃者が”人質”の暗号化されたファイルを本当に複合化してくれるか否かもわからず、恐らくは更なるランサムウェア攻撃を仕掛けるであろうことを防ぐ保証は何もないのです。



マルウェア 分類別割合、2019 年 6 月

私たちは、2019 年 6 月初めから Emotet のフィッシング攻撃の活動が休止しているのに気づきました。 セキュリティ調査グループの Cryptolaemus が、Emotet の最上位のコマンド&コントロール（C2）インフラストラクチャが 6 月 7 日にオフラインになっていることを認識しました。 さらに CenturyLink は、Emotet の C2 インフラストラクチャの構造について、ネットワークの分析調査を使った有用な調査結果を発表しました。 私たちは、組織化された犯罪グループに関する英国のサイバーセキュリティセンターのこれまでの調査結果と合わせて、Emotet のようなマルウェア配信者のビジネスモデルを今後のレポートで精査していきます。



グループ A がグループ B のバンキング系トロイの木馬を配信する場合における「サービスとしてのマルウェア（MaaS）」のビジネスモデル

従来、クリプトマイニングのマルウェアは、深刻度の低い脅威とみなされてきましたが、Bromium の研究室は、Monero を標的にしたクリプトマイニングマルウェアがこの評価を覆すものであると分析しました。 このマルウェアで注目すべきは、Mimikatz や Smbtouch-Scanner、masscan、ProcDump など、公に利用できる侵入後の悪用のツール一式を忍び込ませることができる点です。 こうしたツールを使用しているということは、クリプトマイナーを仕掛けるだけが攻撃者の目的ではないということを示唆しています。 クリプトジャック攻撃が犯罪者にとって魅力的なものになりつつある背景には、暗号通貨の価値の上昇があります。 Monero の価額は、2019 年の上半期の間に 46 ドルから 98 ドルへと 2 倍以上になりました。

注目すべき技術

Bromium の研究室は、政府関連のユーザ企業に共有いただいた悪意によるリッチテキスト形式（RTF）ファイルを、Bromium Secure Platform が隔離した後で分析しました。 このファイルには Windows 10 で Antimalware Scan Interface（AMSI）を回避するための C#のクラスが含まれていました。 AMSI は、サービスや PowerShell のようなアプリケーションを、システムにインストールされたマルウェア対策ソフトウェアによってスキャンできるようにするインタフェースの標準です。 この回避は、メモリにある AmsiScanBuffer 機能にパッチを当てることによって機能し、長さパラメータがゼロになるようにして、AMSI が空のバッファをスキャンして正常な結果を返すようにするのです。 RTF ファイルは PowerShell Add-Type cmdlet を使い、既にホストにインストールされていた.NET Framework ツール（MITRE ATT&CK IDs: T1500 と T1127）を使ってこのクラスを配信した後で、コンパイルしました。 最終的に、この文書は情報窃取のマルウェアファミリーである Pony を配信しようとしたのです。

```
Byte[] q647b53 = { 0x31, 0xff, 0x90 }; // Create array of patch opcodes (XOR EDI, EDI)
IntPtr fc64639 = Marshal.AllocHGlobal(3); // Allocate of 3 bytes of memory and declare pointer to it
Marshal.Copy(q647b53, 0, fc64639, 3); // Copy patch opcodes to allocated memory
h5dab8d(new IntPtr(jb857dc.ToInt64() + 0x001b), fc64639, 3); // Use RtlMoveMemory to patch AmsiScanBuffer at offset 0x1B
// Since the buffer length parameter of AmsiScanBuffer is stored in EDI, the patch sets its length to zero, resulting in AMSI_RESULT_NOT_DETECTED
```

2019 年 6 月に発見された AMSI C#の回避手段に注釈をつけたもの

Bromium の研究室では、マルウェアが用いていた独創的な言語チェック手口を精査し、第 2 段階のペイロードをダウンロードする前に、特定の OS の言語環境のチェックをする動作を把握しました。 システムの言語を直接チェックするのではなく、二種の独立したマルウェアファミリーが、特定の言語パックに固有であるシステムコマンドの出力の中で、文字列の存在チェックをしていました。

コマンド	出力結果	チェック対象	OS 言語
ping 4.4.4.4 -n 0	“Valeur incorrecte pour l’option -n, plage valide comprise entre 1 et 4294967295.”	l’	フランス語
((Get-WmiObject Win32_OperatingSystem).OSArchitecture -match [char]12499)	“32 ビ” “64 ビ”	ビ	日本語

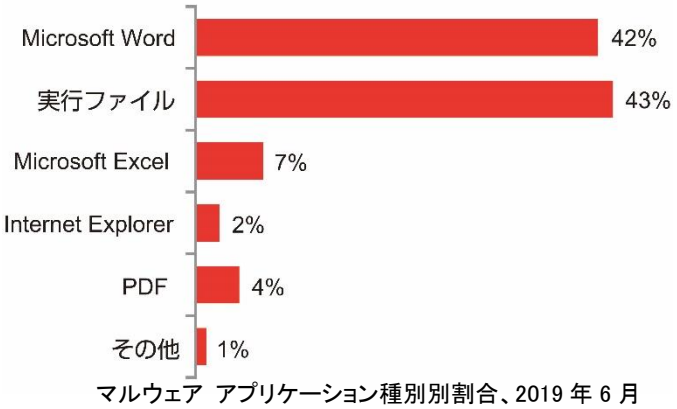
すぐに考慮可能な情報

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 6 月、Bromium のお客様の中で最も多くマルウェアの標的となったアプリケーションは、Portable Executable (PE) 形式のファイルでした。

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。 推奨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。



マルウェア アプリケーション種別別割合、2019 年 6 月

一般的なセキュリティ推奨事項

ユーザがアクセスできるプログラムに最小特権の原則を強制実行することで、攻撃経路を減らすことをお勧めします。 これを実現するには、Windows Defender Application Control（Windows 10、Windows Server 2016、2019）や、Applocker（Windows 7 以降）など、Windows で構築されたアクセス制御機能が使えます。 例えば、リスクの高い環境寄生型のバイナリー（LOLBins）へのアクセスを、組織の中で役割を果たす必要のある Active Directory 内のグループのみに制限することをお勧めします。 また例えば、非開発者のグループは、マルウェアが悪用する可能性のあるツールを構築するアクセス権を持つべきではありません。

シグネチャー

今月のシグネチャーで注目すべきは、言語チェック技術の検出方法です。 下記に、「注目すべき技術」で述べた手口を検出するための OpenIOC シグネチャーを 2 点記載します。

```
<?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="6435ced8-5f43-418b-97d4-6d69a6e78698"
last-modified="2019-07-02T20:44:50" xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>language_check_ping</short_description>
  <description>Detects language-checking technique using ping.exe documented here:
https://www.bromium.com/malware-os-language-targeted-attacks/</description>
  <authored_by>Bromium Labs</authored_by>
  <authored_date>2019-07-02T18:04:03</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="473c0c7f-f76d-4152-a67c-bdbf1ef76edf">
      <IndicatorItem id="ec6bfbd1-46b6-4ed2-97ea-6d213b0d11ad" condition="is">
        <Context document="ProcessItem" search="ProcessItem/name" type="mir" />
        <Content type="string">ping.exe</Content>
      </IndicatorItem>
      <Indicator operator="AND" id="5d3b54d6-c3af-4aa9-969e-0982a81c20fe">
        <IndicatorItem id="d9fb6a8e-763a-4893-bdcc-c52081674687" condition="contains">
          <Context document="ProcessItem" search="ProcessItem/arguments" type="mir" />
          <Content type="string">-n 0</Content>
        </IndicatorItem>
      </Indicator>
    </Indicator>
  </definition>
</ioc>
```

```
<?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="411024cb-350d-4311-b2b7-911cb1adb6ff"
last-modified="2019-07-02T20:44:54" xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>language_check_yakes</short_description>
  <description>Detects language-checking technique used by Yakes documented here:
https://www.bromium.com/malware-os-language-targeted-attacks/</description>
  <authored_by>Bromium Labs</authored_by>
  <authored_date>2019-07-02T20:40:46</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="7cbf6ebd-ecc6-4ab5-a872-1cbb228dd0bf">
      <IndicatorItem id="7e70c36a-2cdf-4442-a7f0-18e2498b1484" condition="is">
        <Context document="ProcessItem" search="ProcessItem/name" type="mir" />
        <Content type="string">powershell.exe</Content>
      </IndicatorItem>
      <Indicator operator="AND" id="4a6d30f8-06a5-4423-beeb-60af42bb306b">
        <IndicatorItem id="2d22628d-f186-4559-9cb6-eec30656c60b" condition="contains">
          <Context document="ProcessItem" search="ProcessItem/arguments" type="mir" />
          <Content type="string">((Get-WmiObject Win32_OperatingSystem).OSArchitecture
-match</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