CloudCoffer

2020 年 8 月 31 日

セキュリティニュース：

狙われるスマホや IoT 機器

今回は CloudCoffer で捕らえたスマホや IoT 機器のマルウェアの事例を紹介します。

スマホ・アプリのケース(2020.8.1):

COVID-19 により多くの人が在宅で仕事をするようになり、企業にとっては追加の脅威にもなっています。

新コロナウイルス対策のための新しい働き方に合わせて、色々な種類の追加的攻撃も行われるようになった昨今、CloudCoffer 製品による検出や同社の調査状況によると、攻撃者が Android 機器用に以前から悪意のある偽のアプリケーション、あるいは普通に期待される機能に届かない悪質な代物を公開しているケースが想定外に多く、被害者がこれらのアプリケーションをインストールするとシステムが危険にさらされる可能性があることがわかっています。

アプリ開発者のほとんどは、セキュリティ上の理由から root 化された Android 携帯電話にユーザがアプリケーションをインストールできないようにコードを記述しています（あるいは、一般ユーザの環境だけで稼働するようにしています）。root 化された携帯電話を持つユーザは、サードパーティからのアプリケーションも利用するなどして、この種のアプリケーションも使用しています。

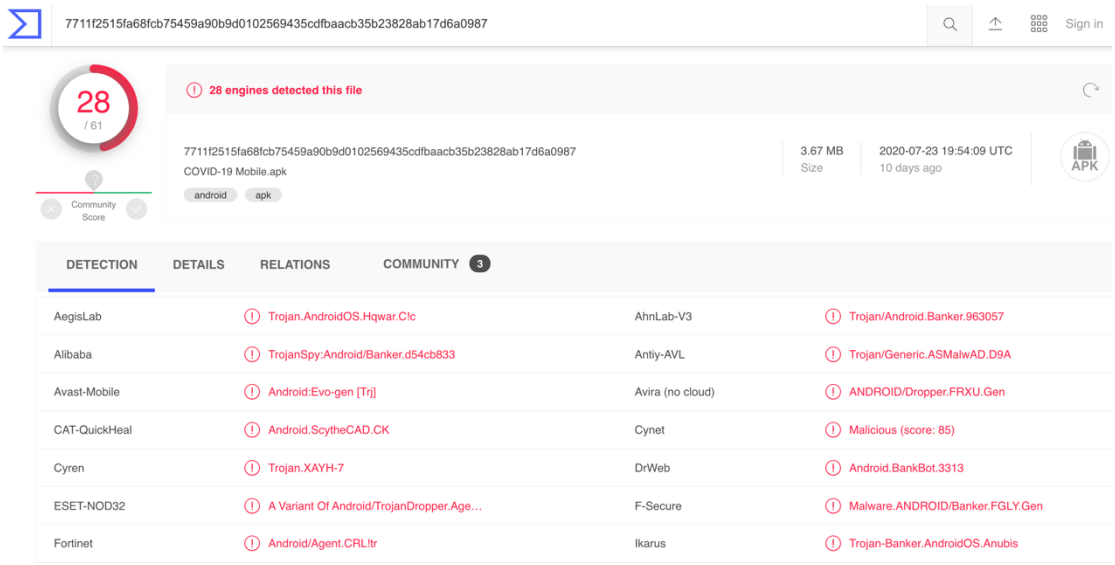
一方サードパーティは、ユーザがデバイスを root 化の有無にかかわらず自社のアプリケーションは普通に使用できる、と主張するかもしれません。そうした時に悲劇が起こります。

CloudCoffer は、サードパーティからのソフトウェア内部に多くの悪意あるコードが隠されていることを発見、解析しています。よくある例としては、BlackRock のファミリーが挙げられます。（参照 日本語解説サイト）

これらのコードは、ユーザがキー入力した機密情報やワンタイムパスワードさえも盗むことができます。多くの C&C サーバはクラウド上にあり、感染した機器からの機密情報 I のアップロードを待っています。この種の攻撃は大惨事を引き起こす可能性があります。

また、同様な仕掛けを使った Android 向けのトロイの木馬も見つかりました。なんとその名は「 COVID-19 Mobile 」です。ユーザの行動履歴から推奨行動を示す、厚生労働省の新型コロナウイルス接触確認アプリ（略称は COCOA）のようなアプリもあります。紛らわしい名称にも注意が必要です。

ARIS Advanced Research & Information Service



VirusTotal の評価結果は見ての通り、現在では 28/61 件と、約半数のアンチウイルスがこのマルウェアを検出できますが、ユーザの携帯電話にマルウェアがインストールされている場合、マルウェアが発見される可能性は低いです。（スマホで定期スキャンをしているユーザはどれくらい居るだろうか？ 時々アンチ・ウイルス・ソフトを入れ替える -物好きな- ユーザなど居るだろうか？）

さらに悪いことに、ほんの少しの追加技術でマルウェアの変種を作れば、ほとんどのアンチウイルスは脅威を検出することができません。この事実は、スマホや PC・サーバ用のアンチウイルスでも、WAF などでも共通です。

CloudCoffer は、C&C サーバに機密情報をアップロードするように制御された多くの被害者のシステムを検出してきた実績があります。

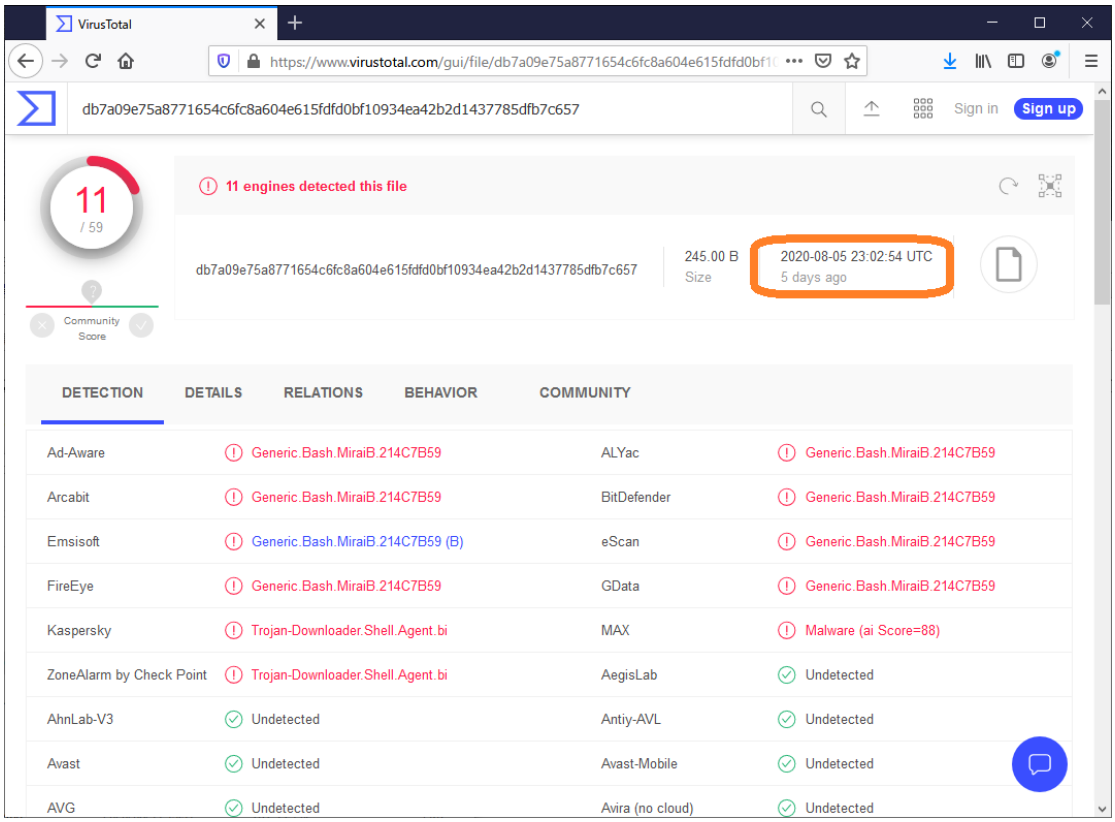
時には、検知したその通信は単に Android アプリのアップデートだった、ということもありましたが、ユーザがアップデートボタンをクリックした時、彼らの機密情報が C&C サーバにアップロードされることも有るわけです。

さらに悪いことに、攻撃者は被害者のシステムを遠隔操作し、これらの感染した携帯電話から企業のネットワークにさらに影響範囲を拡大する可能性があります。

この種のマルウェアを発見した場合の対策と、その労力は想像に難くないでしょうが、発見できない状態で放置されている場合のリスクは重大です。

MIRAI ウイルスもキャッチ：

８月に入ってからでも、あるインストールベースで有名な Mirai ウイルスを検出しました。



VirusTotal サイトでの評価は、11/59 件と、有名なマルウェアである分だけ、検出比も普通のゼロディ物件よりは高くなっています。この図のものは今回の検出で登録した変種で、ユニークなことが分かります。（日付に注意。またファイル名も示されていない）

Mirai ウイルス自体の解説は他有名サイトの情報も十分有用ですが、IoT 機器に棲みついたウイルスが C&C サーバと通信して、特定サイトへのサービス拒否攻撃を一斉に行うという点がユニークで、かつ過去最大級の DoS 通信量を記録し有名どころのインフラ提供側が一度匙を投げた、など数々の話題も提供してきました。

プログラム・ソースも公開されているという事で、2016 年の最初の大攻撃から、色々な攻撃者によって変革し続けていると想定すべきです。これを某社のイントラネット通信で捕らえたという事は、それらの亜種、変種が PC なども利用して随所に拡散している事を窺がわせます。

もともと IoT 機器はエンドポイントのセキュリティソリューションを適用しにくい性質の機器でもあり、ネットワーク上の通信を監視することでセキュリティを監視する CloudCoffer のような製品の適用が求められる分野と言えます。しかも、CloudCoffer なら強力な検知能力を発揮して貴社のセキュリティを充実させる事ができます。

以上、少しでもご参考になれば幸いです。

お問い合わせ先：株式会社アリス　AI セキュリティ事業部<aisec@aris-kk.co.jp>

CCC（CloudCoffer on Cloud）サイト：https://ccc.cloudcoffer.jp

CloudCoffer サイト：https://www.cloudcoffer.jp

RayAegis Japan サイト：https://www.rayaegis.co.jp