2020 年 3 月 19 日

セキュリティニュース：

TICK 攻撃集団に注意！ 通常のシステムでは守れない攻撃マルウェアの実態

2020 年 2 月、ARIS と CloudCoffer は日本の PoC サイトに於いても、TICK 集団からの攻撃が行われている状況を捕捉した。今回も、高度なセキュリティサービスを提供している関連会社である Ray Aegis Information Security ならびにその日本法人レイ・イージス・ジャパンの知見も加え、状況をレポートする。

TICK 集団とは何者か？

TICK は、著名ブランドや軍需、先端機器などのサイトとシステムを極長期間にわたって集中攻撃する中国系の集団である。2020 年になってからも、三菱電機が被害を受けたニュースによってクローズアップされたが、その活動は 10 年以上続いていると報告されている。CloudCoffer の海外顧客サイトでも、リリース間もない 2017 年ほどから攻撃者の一つとして認知されており、注意を要する。また、日本語と日系企業に特化した攻撃が行われていることも分かっている。

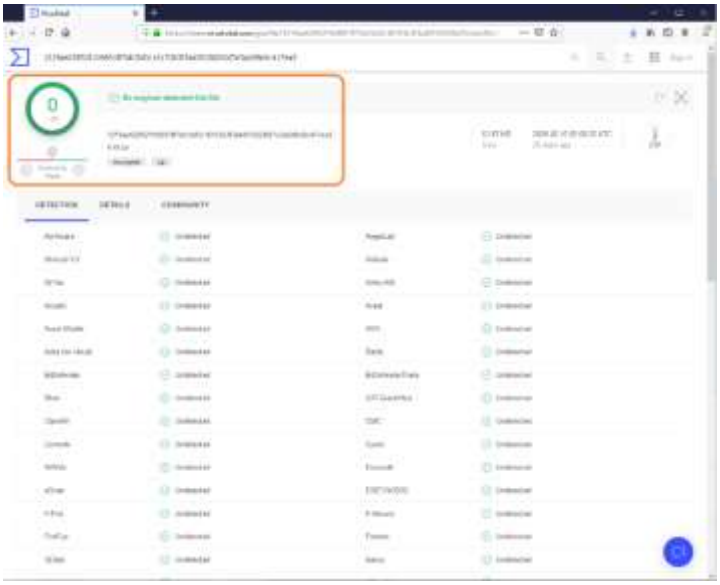
その攻撃手法は良く言えば洗練されていて、既存の保護手段（IPS/IDS/WAF/アンチウィルスなど）をすり抜ける、マルウェアを進化させるなどの手立てが継続的に講じられている。

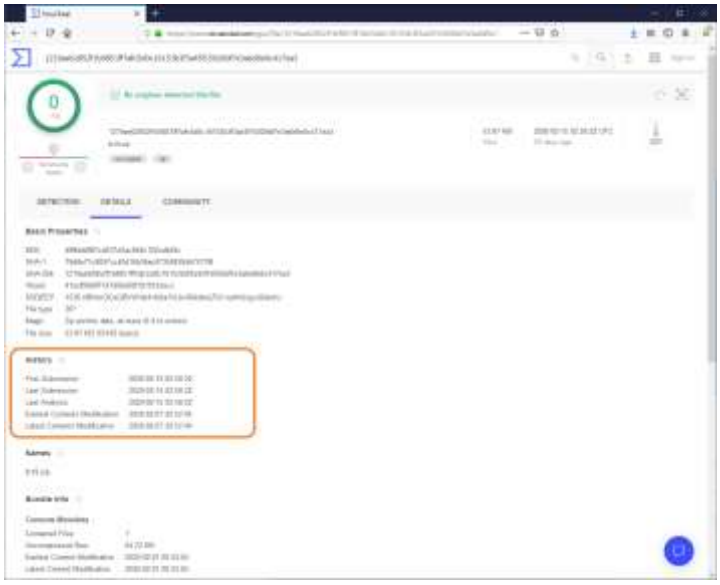
CloudCoffer が発見した TICK のマルウェア

VirusTotal サイトに於いては、58 個のどのウィルスエンジンも検知できない代物である（2020 年 3 月 4 日時点）。CloudCoffer チームは詳細解析の結果、これがゼロデイのマルウェアであると断定している（誤検知ではないと判断している）。

SHA-256:

1219ae62852f1b9851ff7afc5d0c16153b3f3a45f15026bf7e3a6d9e0c417ea3 / 名前: fx19.zip





感染から実行までの手法

CloudCoffer のログ内容から、チームは、この攻撃が次のようになされていることを突き止めた。

- 攻撃者は実在の sanfordbarrows.com から .jpg ファイルをユーザにダウンロードさせる（攻撃者とこのサイトとは無関係だが、既にそこに置いてあった）。
- それを実行可能ファイルに変更して実行する（つまり、ステガノグラフィ技術で隠匿した、実行可能な .jpg ファイルが他社のシステムに埋め込まれていた）。

以上は、該当する一件のログ内容を読み解けば確認できる内容である。

チームはこの検体をダウンロードして解析した。それは何層にも保護されていたが、その実行可能ファイルは一次的な .zip ファイルを生成し、システムに寄生していくことが分かった。

前述のように、fx19.zip は VirusTotal にリストされる、どのアンチウィルス・ソフトでも怪しいとは検知できなかった。

このマルウェアの機能や動作

チームは、この検体について実動作などの追加調査を行った。結果、このマルウェアは実に多くの機能を内在していた。

- シェル環境から OS を制御、設定変更する
- リモートサーバへ接続して、通常とは異なるプロトコルを使って情報を送出する
- イントラネット上の Windows、Linux、mobile OS などのスキャン
- イントラネット内の脆弱なシステムのスキャン。これらで次の犠牲者を探し出す
- 正当なプロセスを kill、自分で偽装して入れ替わる
- 異なるプロトコルでネットワークにアタック（TCP, UDP, ICMP 等であらゆる種類のターゲットを試す）

これらから、最初はシステムをゼロデイ攻撃したり、だましメール（ヒューマン・エンジニアリング手法）などでこの種のマルウェアを埋め込みしたり、長期にわたる攻撃を行っていることが看て取れる。広くインターネット上を調べれば、彼らがそこで使う一連のツールも、多段階にいくつも呼び込まれる事例が多数報告されている。

マルウェアのさらなる解析

このマルウェアの正体を突き止めるため、さらに逆アセンブルなども行い、特徴的な文字セット、文字列（日本語と簡体中国語）なども検出できた。

これらの機能、HTTP 要求のソース IP アドレス、難読化技術などは TICK のものと同じだった（ただし、何年か前に発見されたものとは、既に異なる機能や内容になっている）。

バイナリ内にあるマルウェアのコンパイルパス文字列が TICK の攻撃と同一だった。（UPX：Ultimate Packer for eXecutables をソース入手して多段階に複数の手法でパッキングしてあると想定できる）

TICK 集団のツールと特徴

このマルウェアは、アップデートすることが可能な構造になっている。また取得した機密情報を特定の URL に送付する機能を有する（いわゆる C&C サーバ／C2 サーバを使っている）。

TICK はマルウェアを作り上げることに長けていて、さらには、検知を免れるようなパッケージングを得意としている。

また、次の理由で長い期間発見されずに居られる設計にもなっている。

- 複数の仕組み、システム、サイト（この例の様に本来、無関係なものも使う）などを色々使い、時間をかけて継続的に攻撃している

- 高度に難読化され巧妙にパッケージされていたため、アンチウィルス・ソフトなどでの検知はほぼ不可能（アンチウィルスや WAF などの弱点をよく研究していて、それを破る技術を開発している）
- トリガーのかかるタイミングやコマンドをじっと待っているステルス性のマルウェア
- この例でもアンチウィルス製品にとっては、過去に遭遇したことのない新しいタイプのマルウェアになっている
- 攻撃の成功確率を高めるため、既知・未知のマルウェアを作ったり、複数の OS 環境用のファイルを作成して寄生する

つまり、侵略されたシステム上での動きも巧妙である。これらの結果、不正ファイルが作成された後の孫・子ファイルのスキャンによって初めて検出される、新しいポートが開かれる、などの後段のステップの異常事象が発生するまで、気づかれない事態が発生している。

どうすれば守れるか？

過去の TICK 集団による攻撃も大きな波紋を起こした。その時点の対策を現状環境に適用する場合でも綿密な調査と広範囲の対策が必要である。 このような高スキルで悪意ある集団からの攻撃に対しては VirusTotal サイトに登録されている製品の各種技術では対応できないし、対策に時間が掛かるのも暴露されたことになる。（検知エンジン数が漸増もせず、0 件のままである）

係る状況では、「システムになるべく早く、頻繁に脆弱性対策を行って予防を万全にし、かつ、継続的に異常事象の観測／捕捉を自動化して必要な対策を行う。」という基本的なセキュリティ対策を充実させるくらいしかないと思われる。

しかし、この状況は、「その様にした積りでも気休めでしかない。」という言い方も可能である。

「わが社は、ブランドバリューや、もしもの時の想定被害額からみて、当分静観して置いても良い／して置くしかないだろう。」とお考えのご担当者はおられないだろうか？ 本当にそれで大丈夫でしょうか？

これと同等な対策を、単独のシステムで実現できる「CloudCoffer は即戦力のセキュリティ・コンサルタント」足り得るソリューションと言えるのではないだろうか？

尚、彼らの攻撃について、より広範な内容をカバーしたホワイトペーパーも近日刊行予定です。