雰囲気でインシデントレスポンスをやっている話

drmn

2022 年 2 月 26 日

本来考えていた目次

- 雰囲気でやっている話 #1: 巨人の肩に乗る ← 今日はこれだけ
- 雰囲気でやっている話 #2: 攻撃者の息吹を感じる
- 雰囲気でやっている話 #3: 未知との遭遇

どこで何をやっているのか

セキュリティベンダでコンサルタントとしてインシデント調査を行っています

- 標的型攻撃への対応がメイン
- 年がら年中技術的な調査

雇用主の意見を述べるものではありません

どこで何をやっているのか

セキュリティベンダでコンサルタントとしてインシデント調査を行っています

- 標的型攻撃への対応がメイン
- 年がら年中技術的な調査

雇用主の意見を述べるものではありません

- この LT は特に

たくさんのアーティファクト

フォレンジックの類の調査を行っていると、さまざまなアーティファクトを目にすることになる
例えば Windows システムの調査の場合:

- ファイルシステム (NTFS: MFT, INDX, UsnJrnl, などなど)
- レジストリベースのアーティファクト
  - AppCompat (ShimCache)
  - ShellBag
  - 特に重要なもの (Run キーなど)
  - しばしば重要なもの (アプリケーションの設定や履歴など)
- イベントログ
- その他いろいろ
  - プリフェッチ
  - LNK ファイル
  - ブラウザ履歴

アーティファクトの理解度

1. 調査に使える
   - 使っているツールが結果を提供してくれればそれを調査に役立てることができる
   - アーティファクトの概要、意味合い、ツールの出力結果がわかる

アーティファクトの理解度

1. 調査に使える
   - 使っているツールが結果を提供してくれればそれを調査に役立てることができる
   - アーティファクトの概要、意味合い、ツールの出力結果がわかる
2. 自信を持って使える
   - アーティファクトが提供する情報の詳細を理解している
   - 普段使っているツールがそれをサポートしていない場合でも臨機応変に必要なツールを導入できる
   - 関連する OS, アプリケーションの挙動をよく理解している

アーティファクトの理解度

1. 調査に使える
   - 使っているツールが結果を提供してくれればそれを調査に役立てることができる
   - アーティファクトの概要、意味合い、ツールの出力結果がわかる
2. 自信を持って使える
   - アーティファクトが提供する情報の詳細を理解している
   - 普段使っているツールがそれをサポートしていない場合でも臨機応変に必要なツールを導入できる
   - 関連する OS, アプリケーションの挙動をよく理解している
3. チョットワカル
   - 俺が作った

1 と 2 の間くらいの理解があればだいたいの仕事はできる

例: プリフェッチ

Windows OS がプログラム起動時のパフォーマンスを向上するために、プログラム起動から 10 秒間くらいに読み込まれたファイルを記録しているもの。これがフォレンジック調査にも有用。`%SystemRoot%\Prefetch` フォルダに `.pf` ファイルとして保存

- 例: `CALC.EXE-0FE8F3A9.pf`
  - `0FE8F3A9` の部分は実行ファイルの置かれたパスから計算されたハッシュ値
  - 引数は無視する
    - しかし例外が: `rundll.exe`, `mmc.exe`
    - 新しい OS バージョンでは `dllhost.exe`, `svchost.exe`
- ワークステーション OS では有効だがサーバ OS では無効
  - ワークステーション OS でもディスクが SSD だと無効
  - サーバ OS でも OS 起動時のプリフェッチ `NTOSBOOT-B00DFAAD.pf` だけは存在

例: プリフェッチ

- プリフェッチファイルの存在はそのプログラムがシステム上で実行されたことの証拠となる
- プリフェッチファイルの作成時刻は当該プログラムが最初に実行されたおおよその時刻を示唆する
- ファイルの中身
  - たまに攻撃者がアクセス・実行したデータファイルやスクリプトファイルの手がかりになる
  - プログラムが最後に実行された時刻が記録されている
    - 新しい OS バージョンでは合計直近 8 回分の実行時刻が記録されている
- などなど

人間の限界

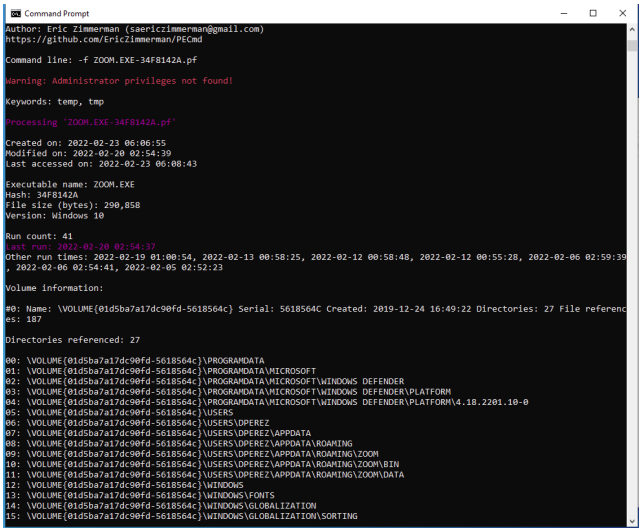
全容を把握するのはつらい

人間の限界

全容を把握するのはつらい
のでツール (パーサ) の助けを借ります

- Eric Zimmerman 氏のツール群
  (`https://ericzimmerman.github.io/`)
- Endpoint Detection and Response (EDR) ソリューション
- 数多のツール

例: Eric Zimmerman 氏の PECmd



プリフェッチファイルから得られる情報を人間にわかりやすい形で提示してくれる

- Created/Modified/Last accessed
- Last run
- Other run times
- アクセスされたファイル

ツールが出力してはじめて気になってくる情報もある

巨人の肩に乗る

それぞれのアーティファクトをしっかりと理解していることは素晴らしい

- そういうものに わたしは なりたい

巨人の肩に乗る

それぞれのアーティファクトをしっかりと理解していることは素晴らしい

- そういうものに わたしは なりたい

そのレイヤでなされた仕事を前提として、次のレイヤの視点からそれを利用することで得られる結果も大きい

- 科学や IT の常套手段

この分野はツールを使いこなすことの重要性が特に大きいように思います

おしまい