初動対応用保全ツール CDIR Collector ユーザガイド

サイバーディフェンス研究所 2022/06/02

1. はじめに

本文書は初動対応用保全支援ツール CDIR Collector のユーザガイドです。CDIR Collector を使って以下のデータを取得することが可能です。

- メモリ
- NTFS 管理ファイル
  - $MFT
  - $SECURE:$SDS
  - $UsnJrnl:$J
- プリフェッチ
- イベントログ
- レジストリ
  - Amcache.hve
  - SAM, SECURITY, SOFTWARE, SYSTEM
  - NTUser.dat, UsrClass.dat
- WMI
- SRUM
- Web(ブラウザ)
  - History (Chrome)
  - cookies.sqlite, places.sqlite (Firefox)
  - WebCacheV01.dat (IE, Edge)
  - History (Edge)
- Windows.old フォルダ内の上記データ (フォルダが存在する場合)

CDIR Collector の実行には対象 PC 上の管理者権限(Administrators)が必要です。

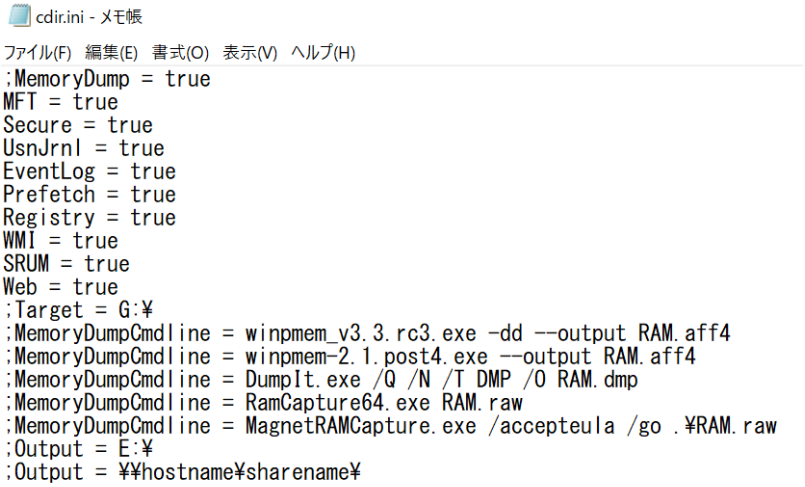
以下の手順は CDIR Collector v1.3.6、Windows 10 日本語版(64bit)の環境で、USB デバイスを使った方法を記載しています。OS のバージョンの違いや設定状態によって、表示内容や項目の名称等が異なる部分があります。

2. 事前準備

CDIR Collector プログラムの配置およびデータの保全場所として USB デバイスを使用します。収集対象のメモリ搭載サイズを上回る容量の媒体を用意してください。

解析用の PC 等を用いて、以下の手順で CDIR Collector の実行用媒体を作成します。

1. USB デバイスを NTFS でフォーマットします。
2. CDIR Collector を以下の URL からダウンロードします。
   https://www.cyberdefense.jp/download/cdir-collector_**バージョン**.zip
3. 入手した CDIR Collector(cdir-collector_**バージョン**.zip)を USB デバイスに保存し、ZIP を展開しておきます。
4. 必要に応じて展開ファイル内の設定ファイル cdir.ini を編集します。以下は cdir.ini のデフォルト設定です。



MemoryDump から Web までの項目は、それぞれのデータを取得するかを設定します。true を指定すると取得し、false を指定すると取得しません。先頭が「;」から始まっている行はコメント扱いとなり、その行は無視します。項目が設定されていない場合は、プログラム実行時に取得する/しないを入力する必要があります。

Target 項目を有効にした場合、指定したドライブレターをシステムボリュームと見なして動作します。保全したディスクイメージに対して主要なデータのみを CDIR Collector で取り出すことを想定した項目です。

標準では Winpmem 2.0.1 を用いてメモリを取得しますが、MemoryDumpCmdline 項目を有効にすると、指定した内容をコマンドとして実行しメモリを取得します。コメント扱いで他のメモリ取得プログラムを利用する場合の設定例を記載しています。Winpmem 以外のメモリ取得プログラム本体は別途入手してください。

Output 項目を設定すると、取得データを CDIR Collector プログラムを実行した場所ではなく、設定したフォルダ配下に保存します。

3. 実行手順

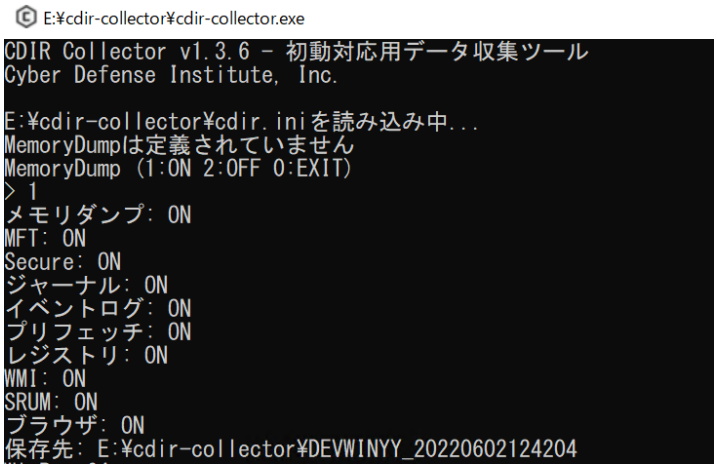
収集対象の PC 上で、以下の手順に従いデータを保全します。

1. 対象 PC に未ログイン状態であればログオンし、CDIR Collector が入っている USB デバイスを接続します。

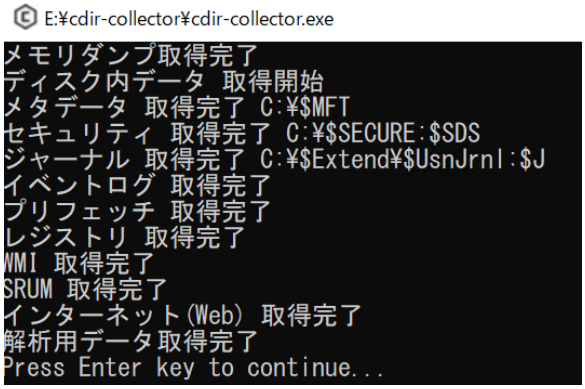
2. USB デバイスに割り当てられたドライブレターを参照し、cdir-collector.exe をダブルクリックします。

3. 設定によってはユーザーアカウント制御のウインドウが現れます。標準アカウントでログインしている場合は管理者アカウントのパスワード入力を求められます。内容を確認し、OK をクリックします。

4. CDIR Collector の実行用ウインドウが表示されます。デフォルト設定ではメモリダンプを取得するか入力を求める状態となるため、メモリダンプを取得する場合は 1 を、メモリダンプの取得をスキップしてディスク上の主要データを取得する場合は 2 を入力します。



5. データ取得処理の開始後、「Press Enter key to continue...」と表示されると完了です。Enter キーを入力してウインドウを閉じてください。



6. CDIR Collector を実行した場所(cdir.ini で Output 項目を設定した場合はその場所)に「**コンピュータ名_実行日時**」のフォルダが存在し、そのフォルダ内に以下のように複数のファイル、フォルダが生成されていることを確認します。

7. 右下のタスクバーから USB デバイス用のアイコンをクリックして、CDIR Collector が入っている USB デバイスを取り出します。

以上で作業は完了です。

なお、ウイルス対策ソフトが常駐していると、本プログラムを脅威として誤検出する可能性があります。その場合はウイルス対策ソフトによる保護を一時的に解除してから実行し、データ取得後に保護を再開してください。