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 2017/04/03

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
- MFT
- UsnJrnl
- プリフェッチ
- イベントログ
- レジストリ
- Web(ブラウザ)

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 v1.2.1、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 プログラムの格納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。

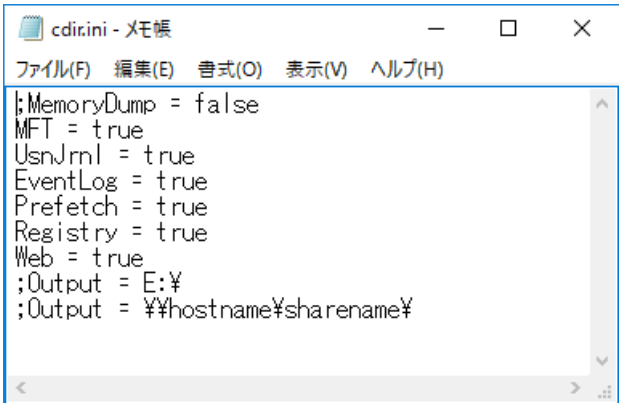
解析用の PC 等を用いて、以下の手順で CDIR Collector の実行用媒体を作成します。

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.zip
3. 入手した CDIR Collector(cdir-collector.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。

   cdir.ini はデータ別に取得の ON/OFF を切り買えるための設定ファイルです。それぞれの項目で 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。

   Output 項目を設定すると、収集データを 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

   以下は cdir.ini のデフォルト設定です。

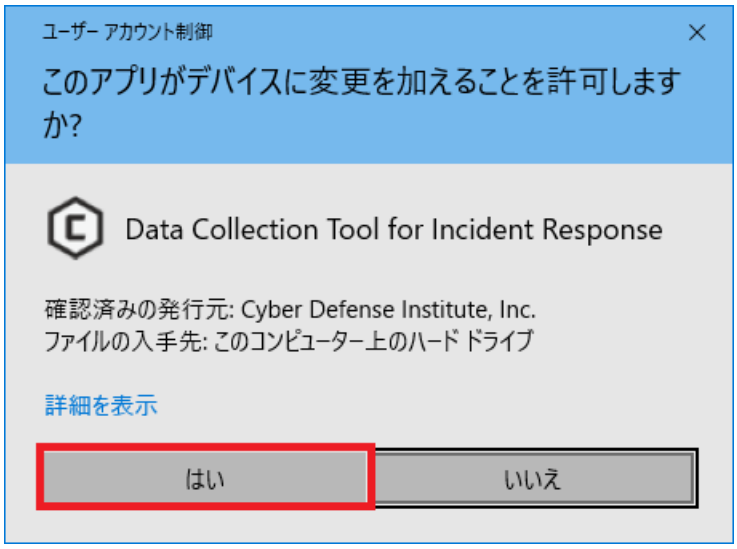


3. 実行手順

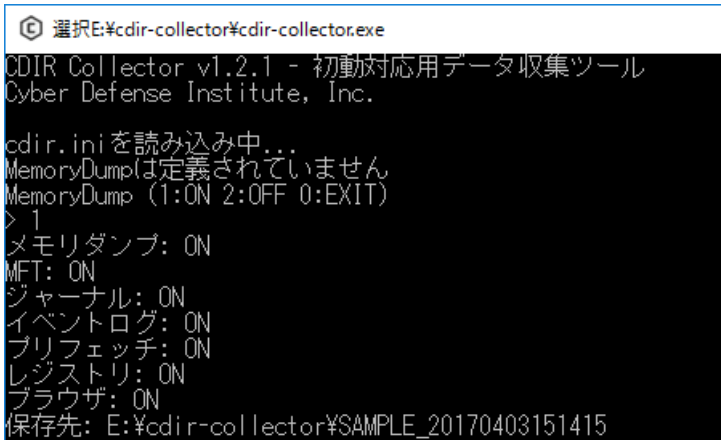
収集対象の PC 上で、以下の手順に従いデータを保全します。

1. 対象 PC に未ログイン状態であればログオンします。
2. 可能であればウイルス対策ソフトの保護を一時的に解除します。
3. CDIR Collector が入っている USB デバイスを対象に接続します。
4. 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。

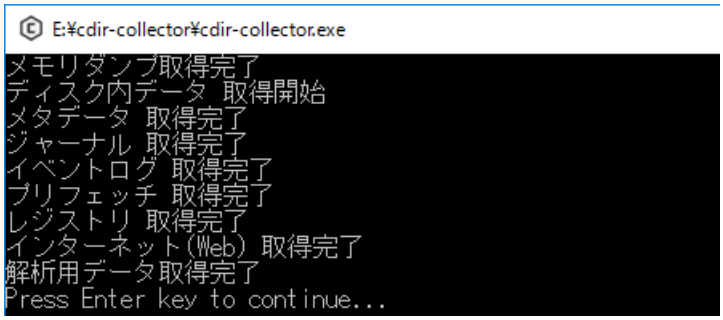
5. 設定によってはユーザーアカウント制御のウインドウが現れます。標準アカウントでログインしている場合は管理者アカウントのパスワード入力を求められます。内容を確認し、OK をクリックします。



6. CDIR Collector の実行を示す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。



7. 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。



8. 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。

9. 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。

10. ウイルス対策ソフトを停止していた場合は保護を再開してください。

以上で作業は完了です。