### reg-bam-entries

Windows 10（ビルド1709以降）のBAM（Background Activity Moderator）がSYSTEMレジストリハイブファイルに記録したデータから、アカウントごとのプログラム実行痕跡を抽出します。

#### 構文

reg-bam-entries [zipcharset=CHARSET] [zippath=ZIPFILE\_PATH] FILE\_PATH

必須パラメータ

**FILE\_PATH**

レジストリファイルのパス。ファイルパスにワイルドカード（\*）を使用すると、パターンに一致するすべてのファイルを一括で検索できます。zippathオプションと併用する場合は、ZIPファイル内に含まれるレジストリファイルのパスを指定してください。

オプションパラメータ

**zipcharset=CHARSET**

ZIPエントリのエンコーディング形式（デフォルト：utf-8）。下記ドキュメントに登録されているPreferred MIME NameまたはAliasesを使用してください: <https://www.iana.org/assignments/character-sets/character-sets.xhtml>

**zippath=ZIPFILE\_PATH**

ZIPファイルのパス

#### 説明

コマンド実行後に出力されるフィールドの内容は、以下の表を参照してください。

**出力フィールド**

|  |  |  |  |
| --- | --- | --- | --- |
| フィールド | 型 | 名称 | 説明 |
| \_file | 文字列 | レジストリハイブファイル名 | 例: SYSTEM |
| sid | 文字列 | プログラム実行アカウントのSID | 例: S-1-5-18 |
| file\_name | 文字列 | 実行ファイル名 | 例: cmd.exe |
| file\_path | 文字列 | 実行ファイルパス | 例: \Device\HarddiskVolume4\Windows\System32\cmd.exe |
| last\_execution | 日付 | 最終実行日時 |  |

#### 使用例

Windows 10のSYSTEMハイブファイルからBAMアーティファクトを抽出

reg-bam-entries D:\data\registry\SYSTEM