### wmi-objects-data

WMI (Windows Management Instrumentation) の OBJECTS.DATA ファイルに保存された CIM オブジェクトを参照します。

#### 構文

wmi-objects-data [zipcharset=CHARSET] [zippath=ZIPFILE\_PATH] FILE\_PATH

必須パラメータ

**FILE\_PATH**

OBJECTS.DATA ファイルのパス。通常は C:\WINDOWS\system32\wbem\Repository\OBJECTS.DATA に配置されています。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 OBJECTS.DATA 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）。以下のドキュメントに記載された 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 | ストレージファイル名 | 例: OBJECTS.DATA |
| \_time | 日付 | 時刻 |  |
| record\_type | 文字列 | レコードタイプ | 例: CLASS\_DEFINITION, INSTANCE\_OBJECT, REGISTRATION |
| class\_name | 文字列 | クラス名 | 例: Win32\_PageFileSetting |
| date1 | 日付 | 日付1 |  |
| date2 | 日付 | 日付2 |  |
| hash | 文字列 | ハッシュ値 |  |
| index\_key | 文字列 | インデックスキー |  |
| instance\_name | 文字列 | インスタンス名 | 例: Connection, provider |
| name | 文字列 | 名前 | 例: CIM\_Setting |
| properties | マップ | プロパティ一覧 |  |
| qualifiers | マップ | 限定子一覧 |  |
| strings | 配列 | 文字列リスト |  |
| super\_class\_name | 文字列 | スーパークラス名 | 例: \_\_SystemClass, \_\_Provider, \_\_Event |

#### 使用例

WMI サブスクリプションを利用した実行検知（T1546.003）

wmi-objects-data C:\windows\system32\wbem\Repository\OBJECTS.DATA | eval strings = strjoin("\n", strings) | search in(strings, "\*\_\_EventFilter\*", "\*\_\_EventConsumer\*", "\*\_\_FilterToConsumerBinding\*")