Remediation

1. Run our script “get\_wmi\_info.ps1” Graphical user interface, application, Word

   Description automatically generated
2. Open remove\_miner.bat file USING NOTEPAD
3. Open ClassesInDefault.txt and take note of any names that contain the modules described above. In our case, the Name of the malicious class is “systemcore\_Updater8”

Text

Description automatically generated

1. Edit Line 9 and Line 18 of remove\_miner.bat to the Name of the malicious WMI Class

Text, application

Description automatically generated

1. Look at EventConsumer.txt, take note of the name of any entries that contains powershell commands encoded in base64 (Sample shown below)   
   (In this case, would be SCM Event8 Log Consumer 2)

Text, application

Description automatically generated

1. Change line 23 of bat file to the Name without the trailing number.

A picture containing text

Description automatically generated

1. Open FilterToConsumerBinding.txt, Recall the names found in Step 5 & 6 (SCM Event8 Log Consumer) (Highlighted in Green). This will tell hint to us the name of the EventFilter it is binded to (Highlighted in Red) (In this case, SCM Event Log Filter | SCM Event Log Filter2).

Graphical user interface, text, application, email

Description automatically generated

1. Return to the bat file and edit line 22 to the filters highlighted in red without the trailing number (SCM Event 8 Log Filter)

A picture containing scatter chart

Description automatically generated

1. Then, Replace the last two lines, 24 & 25 with the two names found in step 7

