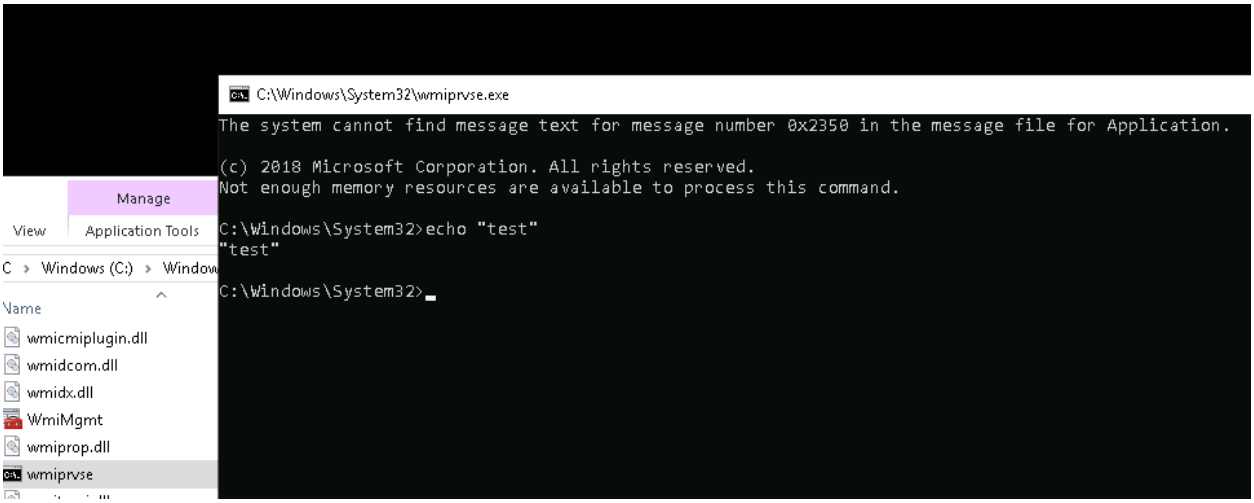
Possible-CobaltStrike-payload-delivery-via-WMI-Edgar

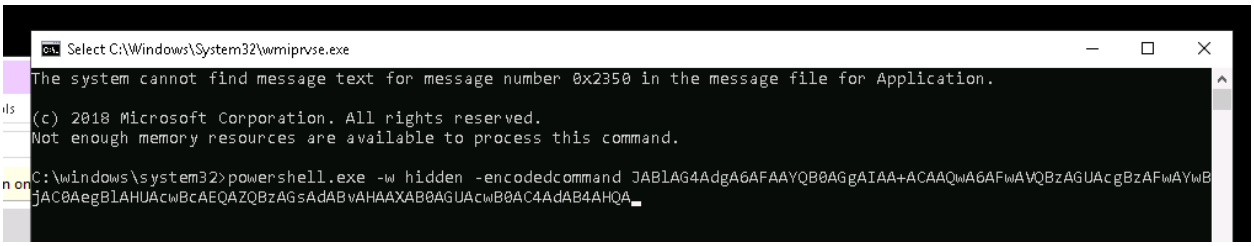
To test this rule I renamed “cmd.exe” to “WmiPrvSe.exe” to be able to get a command prompt as a parent process to launch powershell from it.



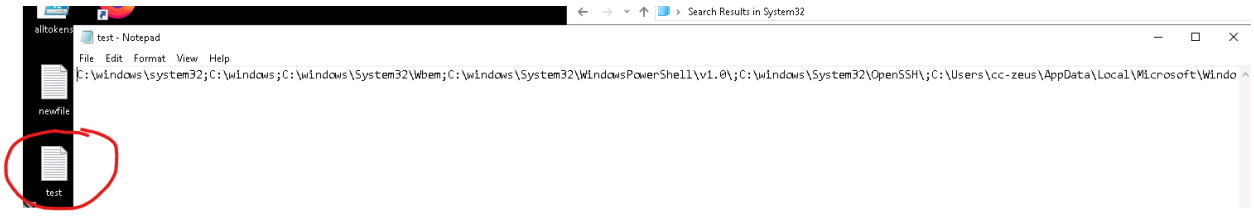
Executed the command line:

powershell.exe -w hidden -encodedcommand JABlAG4AdgA6AFAAYQB0AGgAIAA+ACAAQwA6AFwAVQBzAGUAcgBzAFwAYwBjAC0AegBlAHUAcwBcAEQAZQBzAGsAdABvAHAAXAB0AGUAcwB0AC4AdAB4AHQA

the base64 encoded string decodes to “$env:Path > C:\Users\cc-zeus\Desktop\test.txt'”



Results of the test:



Log in Azure Analytics for the creation of the rule:

EventOriginId	c3ae7f3a-eb28-442b-95d7-af95f503010c
MG	00000000-0000-0000-0000-000000000001
TimeCollected [UTC]	2020-06-25T17:42:39.3Z
ManagementGroupName	AOI-27d04a73-1e5d-46b0-9b1d-885ed1e3547a
CommandLine	powershell.exe -w hidden -encodedcommand JABIAG4AdgA6AFAAYQB0AGgAIAA+ACAAQwA6AFwAVQBzAGUAcgBzAFwAYwBjAC0AegBIAHUAcwBcAEQAZQBzAGsAdABvAHAAXAB0AGU
MandatoryLabel	S-1-16-12288
NewProcessId	0x18f4
NewProcessName	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentProcessName	C:\Windows\System32\wmiprvse.exe
Process	powershell.exe