


51

/ 67



Community Score

 51 security vendors and 4 sandboxes flagged this file as malicious



1814a6a6749684cdacd792374e0ba31b7be4ff6f9675f3fd15d543afbb540367	22.50 KB Size	2021-10-29 10:28:24 UTC 5 days ago
64bits calls-wmi cve-2020-0986 detect-debug-environment exploit peexe		



- DETECTION
- DETAILS
- RELATIONS
- BEHAVIOR
- COMMUNITY 3

 C2AE 

8

### Registry Actions

#### Registry Keys Set

- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\drivers\ndis.sys[MofResourceName]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\System32\Drivers\portcls.SYS[PortclsMof]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\drivers\en-US\ACPI.sys.mui[ACPIMOFResource]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\DRIVERS\HDAudBus.sys[HDAudioMofName]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\System32\Drivers\en-US\portcls.SYS.mui[PortclsMof]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\advapi32.dll[MofResourceName]
- + HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\en-US\advapi32.dll.mui[MofResourceName]





[Sign in](#)[Sign up](#)

+ HKLM\Software\Microsoft\WBEM\WDM\%windir%\system32\drivers\len-US\ndis.sys.mui[MofResourceName]



Registry Keys Deleted

- HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\First Counter
- HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\Last Counter
- HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\First Help
- HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\Last Help
- HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\Object List

Process And Service Actions ⓘ

Shell Commands

%SAMPLEPATH%

Processes Terminated

- %SAMPLEPATH%
- %windir%\System32\svchost.exe -k WerSvcGroup
- %windir%\system32\WerFault.exe -u -p 2664 -s 20
- wmiadap.exe /F /T /R

Processes Tree

↳ 2664 - %SAMPLEPATH%

[Sign in](#)[Sign up](#)

↳ 2732 - %windir%\system32\verr-fault.exe -u -p 2664 -s 20

↳ 2992 - wmiadap.exe /F /T /R

↳ 3028 - %windir%\system32\wbem\wmiprvse.exe

### VirusTotal

[Contact Us](#)[Get Support](#)[How It Works](#)[ToS | Privacy Policy](#)[Blog](#)

### Community

[Join Community](#)[Vote and Comment](#)[Contributors](#)[Top Users](#)[Latest Comments](#)

### Tools

[API Scripts](#)[YARA](#)[Desktop Apps](#)[Browser Extensions](#)[Mobile App](#)

### Premium Services

[Intelligence](#)[Hunting](#)[Graph](#)[API v3 | v2](#)[Monitor](#)

### Documentation

[Searching](#)[Reports](#)[API v3 | v2](#)[Use Cases](#)