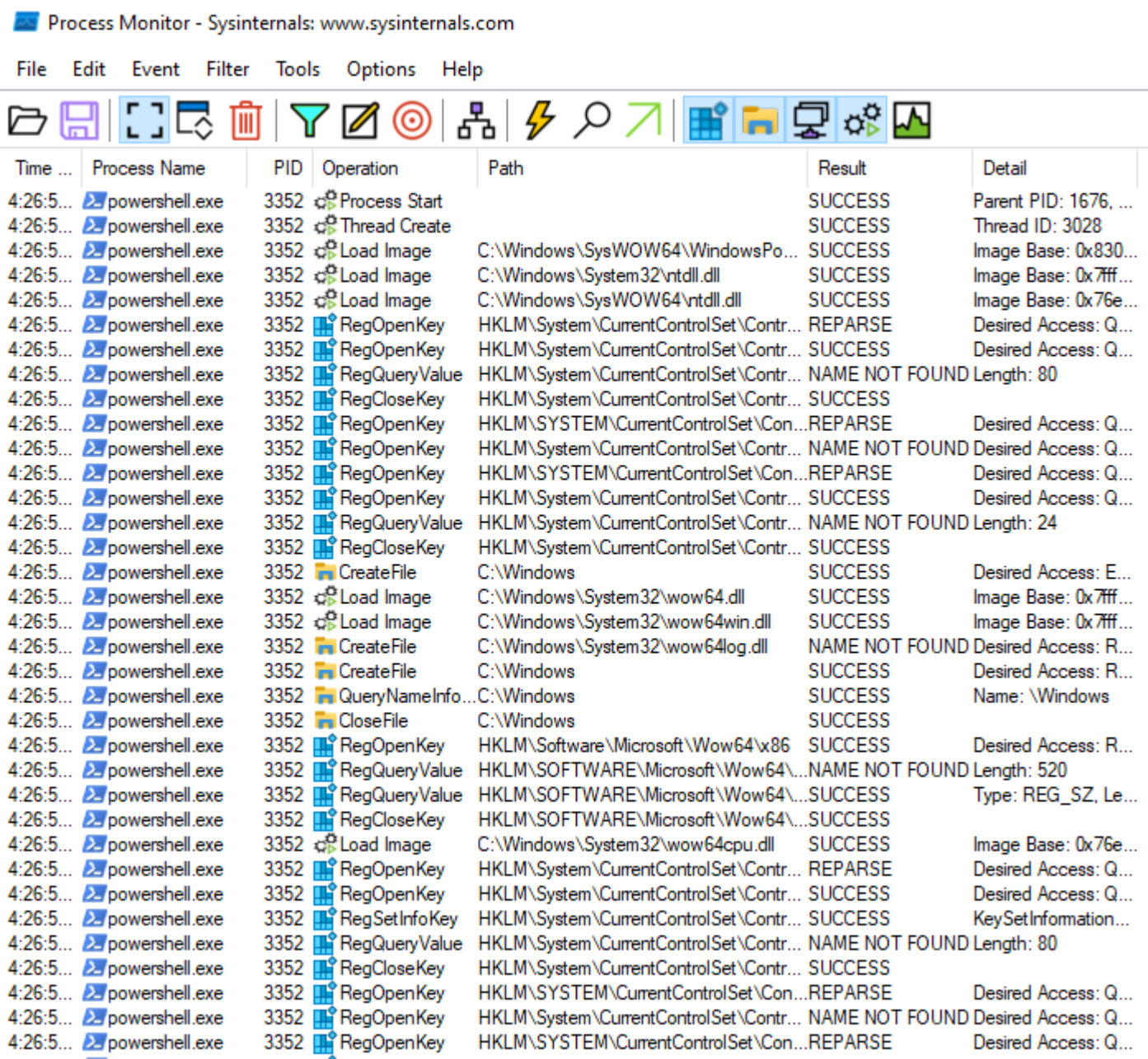
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
4:26:5... powershell.exe 3352 Process Start SUCCESS Parent PID: 1676, ...
4:26:5... powershell.exe 3352 Thread Create SUCCESS Thread ID: 3028
4:26:5... powershell.exe 3352 Load Image C:\Windows\SysWOW64\WindowsPo... SUCCESS Image Base: 0x830...
4:26:5... powershell.exe 3352 Load Image C:\Windows\System32\ntdll.dll SUCCESS Image Base: 0x7fff...
4:26:5... powershell.exe 3352 Load Image C:\Windows\SysWOW64\ntdll.dll SUCCESS Image Base: 0x76e...
4:26:5... powershell.exe 3352 RegOpenKey HKLM\System\CurrentControlSet\Contr... REPARSE Desired Access: Q...
4:26:5... powershell.exe 3352 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...
4:26:5... powershell.exe 3352 RegQueryValue HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Length: 80
4:26:5... powershell.exe 3352 RegCloseKey HKLM\System\CurrentControlSet\Contr... SUCCESS
4:26:5... powershell.exe 3352 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Con... REPARSE Desired Access: Q...
4:26:5... powershell.exe 3352 RegOpenKey HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Desired Access: Q...
4:26:5... powershell.exe 3352 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Con... REPARSE Desired Access: Q...
4:26:5... powershell.exe 3352 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...
4:26:5... powershell.exe 3352 RegQueryValue HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Length: 24
4:26:5... powershell.exe 3352 RegCloseKey HKLM\System\CurrentControlSet\Contr... SUCCESS
4:26:5... powershell.exe 3352 CreateFile C:\Windows SUCCESS Desired Access: E...
4:26:5... powershell.exe 3352 Load Image C:\Windows\System32\wow64.dll SUCCESS Image Base: 0x7fff...
4:26:5... powershell.exe 3352 Load Image C:\Windows\System32\wow64win.dll SUCCESS Image Base: 0x7fff...
4:26:5... powershell.exe 3352 CreateFile C:\Windows\System32\wow64log.dll NAME NOT FOUND Desired Access: R...
4:26:5... powershell.exe 3352 CreateFile C:\Windows SUCCESS Desired Access: R...
4:26:5... powershell.exe 3352 QueryNameInfo... C:\Windows SUCCESS Name: \Windows
4:26:5... powershell.exe 3352 CloseFile C:\Windows SUCCESS
4:26:5... powershell.exe 3352 RegOpenKey HKLM\Software\Microsoft\Wow64\x86 SUCCESS Desired Access: R...
4:26:5... powershell.exe 3352 RegQueryValue HKLM\SOFTWARE\Microsoft\Wow64\... NAME NOT FOUND Length: 520
4:26:5... powershell.exe 3352 RegQueryValue HKLM\SOFTWARE\Microsoft\Wow64\... SUCCESS Type: REG_SZ, Le...
4:26:5... powershell.exe 3352 RegCloseKey HKLM\SOFTWARE\Microsoft\Wow64\... SUCCESS
4:26:5... powershell.exe 3352 Load Image C:\Windows\System32\wow64cpu.dll SUCCESS Image Base: 0x76e...
4:26:5... powershell.exe 3352 RegOpenKey HKLM\System\CurrentControlSet\Contr... REPARSE Desired Access: Q...
4:26:5... powershell.exe 3352 RegOpenKey HKLM\System\CurrentControlSet\Contr... SUCCESS Desired Access: Q...
4:26:5... powershell.exe 3352 RegSetInfoKey HKLM\System\CurrentControlSet\Contr... SUCCESS KeySetInformation...
4:26:5... powershell.exe 3352 RegQueryValue HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Length: 80
4:26:5... powershell.exe 3352 RegCloseKey HKLM\System\CurrentControlSet\Contr... SUCCESS
4:26:5... powershell.exe 3352 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Con... REPARSE Desired Access: Q...
4:26:5... powershell.exe 3352 RegOpenKey HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Desired Access: Q...
4:26:5... powershell.exe 3352 RegOpenKey HKLM\SYSTEM\CurrentControlSet\Con... REPARSE Desired Access: Q...