Process Monitor - Sysinternals: www.sysinternals.com Tools Options File Edit Event Filter Help 유 👂 🔎 🖊 📑 🚍 🕏 🧀 Process Name Path Result Operation Time ... 3352 Process Start 4:26:5... Dowershell.exe SUCCESS

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

Detail

Parent PID: 1676. ...

Desired Access: R...

Type: REG_SZ, Le...

Desired Access: Q... KeySetInformation...

Desired Access: Q...

Desired Access: Q...

4:26:5	powershell.exe	3352	⇔ Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS
4:26:5	powershell.exe	3352	⊯ RegOpenKey	HKLM\System\CurrentControlSet\Contr	REPARSE
4:26:5	powershell.exe	3352	II RegOpenKey	HKLM\System\CurrentControlSet\Contr	SUCCESS
4:26:5	powershell.exe	3352	RegQueryValue	HKLM\System\CurrentControlSet\Contr	NAME NOT FO
1.26.5	Nowarchall ava	2252	RegCloseKey	HKLM\Svetam\CurrentControlSet\Contr	SHICCESS

4:26:5	powershell.exe	3352	₽ů	RegOper	Key	HKLM\System\CurrentControlSet\Contr SUCCESS	Desired Access: Q
4:26:5	powershell.exe	3352	₽ů	RegQuer	yValue	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND) Length: 80
4:26:5	powershell.exe	3352	₽ů	RegClose	Key	HKLM\System\CurrentControlSet\Contr SUCCESS	
4:26:5	powershell.exe	3352	₽ů	RegOper	Key	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired Access: Q
4:26:5	powershell.exe	3352	T.º	RegOper	Key	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND	Desired Access: Q

6:5	powershell.exe	3352	RegQueryValue	HKLM\System\CurrentControlSet\Contr NAME NOT	FOUND Length: 80
6:5	powershell.exe	3352	📫 RegCloseKey	HKLM\System\CurrentControlSet\Contr SUCCESS	
6:5	powershell.exe	3352	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired Acc
6:5	powershell.exe	3352	RegOpenKey	HKLM\System\CurrentControlSet\Contr NAME NOT	FOUND Desired Acc
6:5	powershell.exe	3352	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired Acc

.0.0	poweralien.cxc	JJJ2	m ricgadely value	The May Stell Cultivities and See Continue 1401100110	/ Dongin
6:5	powershell.exe	3352	📫 RegCloseKey	HKLM\System\CurrentControlSet\Contr SUCCESS	
6:5	powershell.exe	3352	⊯ RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired
6:5	powershell.exe	3352	⊯ RegOpenKey	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND) Desired
6:5	powershell.exe	3352	⊯ RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired
6:5	powershell.exe	3352	RegOpenKey	HKLM\System\CurrentControlSet\Contr SUCCESS	Desired

6:5	powershell.exe	3352 🎬 RegCloseKey	HKLM\System\CurrentControlSet\Contr SUCCESS	
6:5	powershell.exe	3352 🏬 RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired
6:5	powershell.exe	3352 🏬 RegOpenKey	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND	Desired
6:5	powershell.exe	3352 🏬 RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired
6:5	powershell.exe	3352 🏬 RegOpenKey	HKLM\System\CurrentControlSet\Contr SUCCESS	Desire
6:5	powershell.exe	3352 RegQueryValue	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND	Length

6:5	powershell.exe	3352 RegCloseKey	HKLM\System\CurrentControlSet\Contr SUCCESS	
6:5	powershell.exe	3352 RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE Desired Access: Q	
6:5	powershell.exe	3352 RegOpenKey	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND Desired Access: Q	
6:5	powershell.exe	3352 RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE Desired Access: Q	
6:5	powershell.exe	3352 RegOpenKey	HKLM\System\CurrentControlSet\Contr SUCCESS Desired Access: Q	
6.5	27 powershell exe	3352 RegQueryValu	e HKLM\Svstem\CurrentControlSet\Contr NAME NOT FOUND Length: 24	

	DO ITOTOTION.ONG	0002	m riogolocolito,	The control of the co	
6:5	powershell.exe	3352	II RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired
6:5	powershell.exe	3352	II RegOpenKey	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND	Desired
6:5	powershell.exe	3352	II RegOpenKey	HKLM\SYSTEM\CurrentControlSet\ConREPARSE	Desired
6:5	powershell.exe	3352	II RegOpenKey	HKLM\System\CurrentControlSet\Contr SUCCESS	Desired
6:5	powershell.exe	3352	RegQueryValue	HKLM\System\CurrentControlSet\Contr NAME NOT FOUND	Length
			A		

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
4.20	· E Maauuamball ava	2252 **	Öl and Image	C:\\Mindows\Custom22\useuC4 dll	CHCCECC	Impac Dage: 0.7ff

4:26:5	powershell.exe	3352	RegCloseKey	HKLM\System\CurrentControlSet\Contr	SUCCESS	
4:26:5	powershell.exe	3352	Create File	C:\Windows	SUCCESS	Desired Access: E
4:26:5	powershell.exe	3352	Ç [©] Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7fff
4:26:5	powershell.exe	3352	Ç [©] Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7fff
4:26:5	powershell.exe	3352	Create File	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R

HKLM\SOFTWARE\Microsoft\Wow64\...NAME NOT FOUND Length: 520

HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Length: 80

HKLM\System\CurrentControlSet\Contr... NAME NOT FOUND Desired Access: Q...

HKLM\SOFTWARE\Microsoft\Wow64\...SUCCESS

HKLM\System\CurrentControlSet\Contr... SUCCESS

HKLM\System\CurrentControlSet\Contr... SUCCESS

HKLM\Svstem\CurrentControlSet\Contr... SUCCESS

HKLM\SYSTEM\CurrentControlSet\Con...REPARSE

HKLM\SYSTEM\CurrentControlSet\Con...REPARSE

20.0	powersnell.exe	3302	Ç≽ Load image	C. \Windows\Jystem32\wow64.dii	SUCCESS	image base. ux/iii
26:5	powershell.exe	3352	Change Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7fff
26:5	powershell.exe	3352	🦐 CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R
26:5	powershell.exe	3352	🦐 CreateFile	C:\Windows	SUCCESS	Desired Access: R
26:5	powershell.exe	3352	QueryNameInfo	.C:\Windows	SUCCESS	Name: \Windows

<u>/</u> b:5	z powersnell.exe	3352 © Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image
26:5	powershell.exe	3352 ¢₿Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	lmage
26:5	powershell.exe	3352 🧰 Create File	C:\Windows\System32\wow64log.dll	NAME NOT FOUN	D Desire
26:5	powershell.exe	3352 🙀 Create File	C:\Windows	SUCCESS	Desire

6:5	2 powershell.exe	3352	CC Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image
			Create File		NAME NOT FOUND	
			Create File	C:\Windows	SUCCESS	Desired
6.5	nowershell exe	3352	Query Name Info	C:\Windows	SUCCESS	Name:

	DO THOTOTION.ONG	0002	Wy Load Illiago	o. armidono appromoz aron o minida	0000200	mage .
26:5	powershell.exe	3352	🦐 CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired
26:5	powershell.exe	3352	🦐 CreateFile	C:\Windows	SUCCESS	Desired
26:5	powershell.exe	3352	QueryNameInfo	.C:\Windows	SUCCESS	Name:

4:26:5	powershell.exe	3352	🧰 Create File	C:\Windows	SUCCESS	Desi
4:26:5	powershell.exe	3352	📷 Query Name Info	.C:\Windows	SUCCESS	Nam
4:26:5	powershell.exe	3352	📻 CloseFile	C:\Windows	SUCCESS	
4:26:5	powershell.exe	3352	RegOpenKey	HKLM\Software\Microsoft\Wow64\x86	SUCCESS	Desi

4:26:5	powershell.exe	3352	📻 CreateFile	C:\Windows	SUCCESS	Des
4:26:5	powershell.exe	3352	🙀 Query Name Info	C:\Windows	SUCCESS	Nan
4:26:5	powershell.exe	3352	CloseFile	C:\Windows	SUCCESS	

```
3352 RegCloseKev
                                                  HKLM\SOFTWARE\Microsoft\Wow64\...SUCCESS
4:26:5... Dowershell.exe
                           3352 CLoad Image
                                                                                                       Image Base: 0x76e...
4:26:5... Dowershell.exe
                                                  C:\Windows\Svstem32\wow64cpu.dll
                                                                                      SUCCESS
                           3352 RegOpenKey
                                                                                                       Desired Access: Q...
4:26:5... Dowershell.exe
                                                  HKLM\Svstem\CurrentControlSet\Contr... REPARSE
```

3352 RegQueryValue 3352 RegQueryValue

3352 RegOpenKey

3352 RegSetInfoKey

3352 RegQueryValue

3352 RegCloseKey

3352 RegOpenKey

3352 RegOpenKey

3352 RegOpenKey

4:26:5... Dowershell.exe

4:26:5... Dowershell.exe